NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

INTERPRETIVE ANALYSIS OF THE JOINT MARITIME COMMAND INFORMATION SYSTEM (JMCIS) SENSITIVE COMPARTMENTED INFORMATION (SCI) LOCAL AREA NETWORK (LAN) SECURITY REQUIREMENTS

by

Mark T. Weatherford

September, 1994

Thesis Advisors: Carl R. Jones
Cynthia E. Irvine

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 1994	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE INTERPRETIVE ANALYSIS OF THE JOINT MARITIME COMMAND INFORMATION SYSTEM (JMCIS) SENSITIVE COMPARTMENTED INFORMATION (SCI) LOCAL AREA NETWORK (LAN) SECURITY REQUIREMENTS	5. FUNDING NUMBERS
6. AUTHOR (S) Weatherford, Mark T.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT *(maximum 200 words)*

The primary purpose of this thesis is to provide an analysis for each of the specific security requirements established for the Joint Maritime Command Information System (JMCIS) Sensitive Compartment Information (SCI) local area network. The development of JMCIS and its importance within the interoperability arena of Department of Defense (DoD) Command, Control, Communications, Computers, and Intelligence (C4I) systems is discussed. A description of the components for the SCI local area network and supporting computer security principles is presented. The author employs the criteria established in the Trusted Computer System Evaluation Criteria (TCSEC) and other authoritative sources to evaluate and interpret the security requirements under the broad category of *Technical (Computer) Security Requirements* for the JMCIS SCI local area network. The results of the analysis support the JMCIS SCI local area network developer's selected security requirements.

14. SUBJECT TERMS COE, Computer Security, C4I, interoperability, JMCIS, local area network, SCI, System-High, TCSEC, UB	15. NUMBER OF PAGES 127
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

ABSTRACT

The primary purpose of this thesis is to provide an analysis for each of the specific security requirements established for the Joint Maritime Command Information System (JMCIS) Sensitive Compartmented Information (SCI) local area network. The development of JMCIS and its importance within the interoperability arena of Department of Defense (DoD) Command, Control, Communications, Computers, and Intelligence (C4I) systems is discussed. A description of the components for the SCI local area network and supporting computer security principles is presented.

The author employs the criteria established in the Trusted Computer System Evaluation Criteria (TCSEC) and other authoritative sources to evaluate and interpret the security requirements under the broad category of *Technical (Computer) Security Requirements* for the JMCIS SCI local area network.

The results of the analysis support the JMCIS SCI local area network developer's selected security requirements.

TABLE OF CONTENTS

I. INTRODUCTION 1
A. PURPOSE 1
B. SCOPE 2
C. OVERVIEW OF CHAPTERS 2
1. Introduction 2
2. Joint Maritime Command Information System (JMCIS) 2
3. The Sensitive Compartment Information (SCI) Local Area Network (LAN) 3
4. Computer Security 3
5. Sensitive Compartmented Information (SCI) Local Area Network Security Requirements 4
6. Conclusions 4
II. JOINT MARITIME COMMAND INFORMATION SYSTEM (JMCIS) 5
A. POLICY 5
1. DoD's Corporate Information Management (CIM) 5
2. The Joint Staff's "C4I for the Warrior" 7
3. The Navy's Copernicus Architecture 8
B. SYSTEMS 9
1. Joint Operational Tactical System (JOTS) 10
2. Navy Tactical Command System - Afloat (NTCS-A) 11
3. Operations Support System (OSS) 12
C. JMCIS 12
1. Genesis and History 13
2. System Migration 14
3. What is JMCIS? 15
a. Components of JMCIS 18
(1) Applications 18
(2) Common Operating Environment (COE) 18
(3) Unified Build (UB) 18

(4) Segment 19
(5) Variant 19
(6) GENSER Local Area Network / SCI Local Area Network 19
b. The Three Perspectives of JMCIS 20
(1) Sailor / Soldier Perspective 20
(2) Program Manager Perspective 20
(3) System Developer Perspective 21
D. WHY JMCIS? 21
1. Operational Justification 22
a. Command, Control, Communications, Computers, and Intelligence (C4I) 22
b. Technology Explosion 22
c. Shared Access to Common Data 24
2. Financial Justification 24
a. Configuration Management - Hardware/Software 25
b. Training 25
E. THE JMCIS PHILOSOPHY 26
1. Don't Reinvent the Wheel 26
2. Existing Standards 26
3. Interpretability 27
4. Focus Attention 27
F. THE OBJECTIVES OF JMCIS 27
1. Commonality 28
2. Reusability 28
3. Standardization 28
4. Engineering Base 28
5. Training 28
6. Interoperability 28
7. Certification 29
8. Testing 29
G. THE FUTURE 29

III. THE SENSITIVE COMPARTMENTED INFORMATION (SCI) LOCAL AREA NETWORK 31
A. SENSITIVE COMPARTMENTED INFORMATION (SCI) 31
B. SCI LOCAL AREA NETWORK DESCRIPTION 32
1. Purpose of SCI LAN 32
2. System Description 33
3. Unified Build 35
4. Segments 36
5. Security Functions 37
IV. COMPUTER SECURITY 38
A. WHAT IS COMPUTER SECURITY? 39
1. Secrecy 39
2. Integrity 39
3. Availability 40
B. WHY SECURITY? 41
C. MODES OF SECURITY 42
1. Dedicated Mode 42
2. System-High Mode 43
3. Multilevel Mode 43
D. EVALUATION CRITERIA FOR TRUSTED SYSTEMS 44
1. Background 44
2. Purpose 45
3. Security Policy 45
a. Discretionary Access Control (DAC) 46
b. Mandatory Access Control (MAC) 46
4. The Criteria 47
a. Division D: Minimal Protection 47
b. Division C: Discretionary Protection 47
(1) Class C1: Discretionary Security Protection 47
(2) Class C2: Controlled Access Protection 48

c. Division B: Mandatory Protection 48
(1) Class B1: Labeled Security Protection 48
(2) Class B2: Structured Protection 48
(3) Class B3: Security Domains 49
d. Division A: Verified Protection 49
E. COMMAND AND CONTROL SCENARIO 51
V. SENSITIVE COMPARTMENTED INFORMATION (SCI) LAN SECURITY REQUIREMENTS 54
A. BACKGROUND 54
B. PURPOSE 54
C. TECHNICAL (COMPUTER) SECURITY (TEC_1.0) REQUIREMENTS 55
1. Conceptual Design - TEC_1.1 55
a. Description 55
b. Interpretation and Rationale 55
2. System Architecture - TEC_1.2 56
a. Description 56
b. Interpretation and Rationale 56
3. Discretionary Access Control - TEC_1.3 57
a. Description 57
b. Interpretation and Rationale 57
4. Identification and Authentication - TEC_1.4 59
a. Description 59
b. Interpretation and Rationale 59
5. Single User ID - TEC_1.4.1 60
a. Description 60
b. Interpretation and Rationale 60
6. Password Length - TEC_1.4.2 60
a. Description 60
b. Interpretation and Rationale 60
7. Privileged User Limitation - TEC_1.5 61
a. Description 61
b. Interpretation and Rationale 61

8. Role Change - TEC_1.6 61
a. Description 61
b. Interpretation and Rationale 61
9. Data Base Manager Role - TEC_1.7 62
a. Description 62
b. Interpretation and Rationale 62
10. Menu Item Gray-Out - TEC_1.8 63
a. Description 63
b. Interpretation and Rationale 63
11. Audit - TEC_1.9 63
a. Description 63
b. Interpretation and Rationale 63
12. Minimum Audit Data - TEC_1.9.1 64
a. Description 64
b. Interpretation and Rationale 65
13. Audit User Role - TEC_1.9.2 65
a. Description 65
b. Interpretation and Rationale 65
14. Audit Unsuccessful Log-on Attempts - TEC_1.9.3 65
a. Description 65
b. Interpretation and Rationale 66
15. Message Handling Audit - TEC_1.9.4 67
a. Description 67
b. Interpretation and Rationale 67
16. Log-on Alarm - TEC_1.10 67
a. Description 67
b. Interpretation and Rationale 67
17. Marking Printed Output - TEC_1.11 68
a. Description 68
b. Interpretation and Rationale 68

18. Object Reuse - TEC_1.12 69
a. Description 69
b. Interpretation and Rationale 69
19. Identification of User Terminal - TEC_1.13 70
a. Description 70
b. Interpretation and Rationale 70
20. Automated Guard Processors and Filters - TEC_1.14 70
a. Description 70
b. Interpretation and Rationale 70
21. System Integrity - TEC_1.15 71
a. Description 71
b. Interpretation and Rationale 71
22. Protection of Network Control - TEC_1.16 72
a. Description 72
b. Interpretation and Rationale 72
23. Integrity of Intelligence Data - TEC_1.17 73
a. Description 73
b. Interpretation and Rationale 73
24. Security Markings For Exported Intelligence - TEC_1.18 74
a. Description 74
b. Interpretation and Rationale 74
25. Security Testing - TEC_1.19 75
a. Description 75
b. Interpretation and Rationale 75
26. Trusted Operating System - TEC_1.20 76
a. Description 76
b. Interpretation and Rationale 76
27. DoD Banner - TEC_1.21 77
a. Description 77
b. Interpretation and Rationale 77

28. Session Security Parameter - TEC_1.22 77
a. Description 77
b. Interpretation and Rationale 77
VI. CONCLUSIONS AND RECOMMENDATIONS 79
A. CONCLUSIONS 79
B. RECOMMENDATIONS 80
1. TEC_1.2 and TEC_1.20 81
2. TEC_1.9.3 and TEC_1.10 82
3. TEC_1.12 82
4. TEC_1.16 83
APPENDIX 84
A. DETERMINING PASSWORD LENGTH 84
1. Relationship 84
2. Guess Rate 85
3. Password Lifetime 85
4. Password Space 86
5. Procedure For Determining Password Length 87
6. Example of Password Length Determination 87
REFERENCES 90
LIST OF ACRONYMS 94
GLOSSARY 97
BIBLIOGRAPHY 108
INITIAL DISTRIBUTION LIST 113

ACKNOWLEDGEMENT

I would like to thank my thesis advisors for their time and efforts in helping make this thesis materialize. Professor Carl Jones for his guidance in helping me understand the relevant issues of command and control and especially Professor Cynthia Irvine for her interest and desire to make me think and reflect on the significance of computer security.

A special thank you to my wife Sharon, and my children Marshal and Sienna, whose love, support, and personal sacrifice made my graduate education a success.

I. INTRODUCTION

A. PURPOSE

The Joint Maritime Command Information System (JMCIS) program represents a revolutionary paradigm shift in the evolution of command and control systems. As an umbrella program encompassing various command, control, communications, computers, and intelligence (C4I) systems, JMCIS provides a central pool of operations and planning information to the battlespace commander. The key to the JMCIS concept is migration of legacy "stove-pipe" command and control systems to an open architecture environment based on a common "core" set of software called the Unified Build. This common "core" software enables basic functions to be utilized by all applicable software segments and ensures consistency of processes throughout the system.

The JMCIS concept brings significant advantages to the command and control environment including interoperability among Joint organizations and the DoD, financial savings through the development and use of common software, decreased life-cycle management costs through maintenance of a single system, and implementation of common standards.

B. SCOPE

The objective of this thesis is to provide a detailed examination of the JMCIS concept and the role of the Sensitive Compartmented Information (SCI) local area network. Following the background information on JMCIS and the SCI local area network, an interpretive analysis is presented for each of the specific security requirements developed for the SCI local area network. While there are various areas of security with established requirements, the author specifically analyzes the security requirements under the broad category of Technical (Computer) Security. This thesis will not address issues related to Communications Security (COMSEC).

C. OVERVIEW OF CHAPTERS

1. Introduction

Chapter 1 discusses the purpose and scope of the thesis.

2. Joint Maritime Command Information System (JMCIS)

Chapter II provides a chronological history of DoD policies, various command and control systems, and the progression to the current open architecture environment of JMCIS. Following the history of JMCIS is a general outline of the components of the architecture and justifications, from an operational and financial perspective, of the need to move towards a JMCIS concept. Finally, the philosophy and objectives of JMCIS are presented to validate the need for a design to change the current method of developing command and control systems.

3. The Sensitive Compartment Information (SCI) Local Area Network (LAN)

Chapter III presents a general discussion of the differences in GENSER and SCI information and the necessity for separate, more restrictive access and storage requirements for SCI data. The demand for an SCI local area network, distinct and isolated from the JMCIS GENSER local area network, is justified by the need to add value to the commander's overall tactical picture without disclosing sources of this potentially more sensitive information. Finally, the SCI local area network architecture and the system-high mode of operation are discussed to observe the different operating concepts and procedures as opposed to normal GENSER operations.

4. Computer Security

Chapter IV introduces the concept of computer security and why the increasing use of computers throughout DoD has heightened the need for measures to combat security related problems. Simple access to computer networks is becoming commonplace and the threat of malicious software code introduction into a computer system is growing. As a result, the DoD has developed the Trusted Computer System Evaluation Criteria (TCSEC) as a means to quantify or measure the trust placed in computer systems. The levels of the TCSEC are explained and the increasing assurance associated with each division and class is presented. Finally, a hypothetical scenario is given to illustrate the consequences of enemy exploitation of a command and control system.

5. Sensitive Compartmented Information (SCI) Local Area Network Security Requirements

Chapter V presents the background information necessary to understand the standards used to develop the security requirements for the SCI local area network. The individual requirements established for Technical (Computer) Security are provided, followed by detailed analysis of the requirements. For the individual analysis, multiple sources are used to validate requirements but the primary source is the Trusted Computer System Evaluation Criteria (TCSEC). The TCSEC is the accepted industry standard for trusted systems and its technical evaluation methodologies are well established.

6. Conclusions

Chapter VI provides a conclusion and recommendations to the thesis.

II. JOINT MARITIME COMMAND INFORMATION SYSTEM (JMCIS)

To understand the concept and the philosophy of JMCIS, the external evolutionary and developmental factors must first be examined. Changes in government and Department of Defense (DoD) information management policy and the complexion of the command and control systems absorbed under the JMCIS umbrella are the two defining elements in the evolution of JMCIS.

A. POLICY

The policies that have had the most significant impact in shaping the evolution of JMCIS are DoD's Corporate Information Management (CIM), The Joint Staff's "C4I for the Warrior", and the Navy's Copernicus architecture programs. These policies have contributed to the development of JMCIS by directing the progress of the command and control environment from which it evolved.

1. DoD's Corporate Information Management (CIM)

Defense Management Review Decision (DMRD) 918 provided the initial direction of the Corporate Information Management (CIM) initiative administered by the

---

Chapter II is the product of a collaborative effort between researchers engaged in related JMCIS theses. Contributors include LT Bruce F. Loveless, USN, Capt. Todd F. Sweeney, USMC, and the author.

Defense Information Systems Agency (DISA). CIM is a strategic management initiative intended to guide the evolution of the DoD enterprise by capturing the benefits of the information revolution. It emphasizes both a functional and technical management focus to achieve a combination of improved business processes and effective application of information technology across the functional areas of DoD. It is embodied in policies and programs, implementation guidance, and supporting resources, to help functional managers guide and implement changes to processes, data, and systems across the DoD. [Ref. 1:p. 1]

The management structure of CIM has four "pillars" that support improved Defense capabilities: common information systems; shared, standard data; re-engineered processes; and a computer and communications infrastructure. The overarching goal of CIM is to enable commanders of military forces and managers of support activities to achieve the highest degree of capability in their operations through the effective use of information applied in improved functional processes. The vision of this initiative provides for global end-to-end information connectivity among US and allied forces. In this context, information is considered a critical mission capability and force multiplier for worldwide readiness, mobility, responsiveness, and operations. Joint interoperability and information integration on the battlefield is emphasized to result in significantly improved joint service and multinational operations. [Ref. 1:p. 3]

2. The Joint Staff's "C4I for the Warrior"

C4I for the Warrior is a concept for DoD information management first published by The Joint Staff in 1992. It is clearly targeted at solving the C4I interoperability issues among the services. The intent is to provide an unifying C4I concept that will support the requirements of the joint force Warrior at the battlefield level, while remaining consistent with DoD policy and national security objectives. This focus is expressed by former Chairman, General Colin L. Powell, in the following statement:

> The C4I for the Warrior concept will give the battlefield commander access to all information needed to win in war and will provide the information when, where, and how the commander wants it. The C4I for the Warrior concept starts with the Warrior's requirements and provides a roadmap to reach the objective of a seamless, secure, interoperable global C4I network for the Warrior. [Ref. 2:p. 13]

C4I for the Warrior is considered a seminal doctrine that is intended to guide the evolution of individual service C4I architectures into a broad Global Command and Control System (GCCS). [Ref. 3:p. 49] The concept principles have been incorporated in the Joint Staff's GCCS program.

At the center of the C4I for the Warrior concept is the establishment of a global C4I capability that allows the Warrior to define the battlespace and to "plug in" and "pull" timely, relevant information anytime, anyplace in the performance of any mission. The Warrior, by defining the battlespace, determines the information to "pull" rather than have information "pushed" from various sources. The Warriors neither want nor need the cumulative knowledge of multiple sources dumped into their battlespace information

systems. They want only the specific information they need to win the fight; and they want it when they need it, where they need it, and in the form in which it will do them the most good. This demand pull concept provides the capability for the Warrior to poll the global C4I network for any desired information from any location, at any point in time. This is a key principle of the C4I for the Warrior concept and a guiding concept for future DoD and Navy C4I architecture development.

3. The Navy's Copernicus Architecture

The Copernicus Architecture is the current architectural guidance designed to restructure all Navy C4I systems. The Copernicus Architecture, Phase 1: Requirements Definition, published in 1991, provides both a new C4I architecture to replace the current Navy system and a programmatic investment strategy to construct it over the next decade. [Ref. 4:p. 3-2] It is intended to establish a vision of an overall C4I architecture for the Navy.

The Copernicus Architecture is primarily a telecommunications system designed around a series of global information exchange systems ashore and tactical information exchange systems afloat. The architecture concept is based on four pillars: first, virtual global networks called Global Information Exchange Systems (GLOBIXS); second, metropolitan area networks called CINC Command Centers (CCC); third, tactical virtual nets called Tactical Data Information Exchange Systems (TADIXS); and fourth, interconnecting the previous systems to support the Tactical Command Center (TCC) afloat. In this concept, data can be forwarded from the shored based sensor-to-sensor

infrastructure to the tactical commander's C2 infrastructure afloat. Just as Copernicus brought about a revolutionary paradigm shift in astronomy, the Copernicus Architecture was so named because it represents a revolutionary paradigm shift in command and control systems by being centered on the tactical needs of the operator afloat. [Ref. 5:p. 10-12]

A key operational concept of the Copernicus Architecture is the recognition of the Space and Electronic Warfare Commander (SEWC) as part of the Composite Warfare Commander (CWC) doctrine afloat. This action follows the establishment of SEW as a designated warfare area within the Navy by the CNO in 1989, which doctrinally assigned command and control (C2) functions to the SEW mission. In many ways, this early recognition of the importance of information management for the operational commander served as a building block for further DoD architecture development. The Copernicus goal of establishing a "common operating environment" now is considered part of the Defense Department's "C4I for the Warrior" initiative, which requires the Army, Navy, and Air Force to develop, through a phased process, approaches to making their C4I data-transfer systems fully compatible for joint operations. [Ref. 3:p. 52]

B. SYSTEMS

JMCIS is an umbrella system that has incorporated various functionalities and attributes of previous command and control systems. The philosophy of incorporating other systems capabilities and functionality is not unique to JMCIS, rather it is a trait inherited from previous systems. The Joint Operational Tactical System (JOTS), Navy

Tactical Command System - Afloat (NTCS-A), and Operations Support System (OSS) are examples of systems that applied this same evolutionary methodology and directly influenced the development of JMCIS.

1. Joint Operational Tactical System (JOTS)

JOTS began as a prototyping effort that was first deployed aboard ship in the early 1980s. This system provided the operational commander with the first integrated display of data for decision support purposes. System functionality eventually included track management, track analysis, environment prediction, and a variety of tactical overlays and Tactical Decision Aids (TDAs). JOTS was capable of receiving various data and message input such as Link 11, Link 14, Tactical Data Information Exchange System-A (TADIXS A), Officer in Tactical Command Information Exchange System (OTCIXS), High Interest Track (HIT) Broadcasts, and U.S. Message Text Format (USMTF) messages. JOTS allowed the Fleet Command Centers to interface with command ships and other shore installations. Through the use of a tactical data base manager (TDBM), JOTS provided a consistent tactical battlespace picture for all supporting warfare commanders afloat and ashore. [Ref. 5:p. 60]

The original prototyping effort of JOTS lead to the development of the JOTS Command and Control System by the late 1980s. The primary goal of the JOTS was to integrate information systems onto common hardware and software platforms to provide for the sharing of data bases as well as maximize limited shipboard area. JOTS-derived systems have since been installed onboard over 200 Navy ships, at several US Navy shore

intelligence centers, onboard US Coast Guard vessels, onboard allied ships, and a various allied sites. [Ref. 6:p. 1-1] As JOTS matured further and as other C3I systems were developed and deployed, it became apparent that there was much duplication of software and functionality across systems. This duplication led to increased development, maintenance, and training costs and the stated goal of interoperability across systems was virtually non-existent. This led to low interoperability and most importantly, led to conflicting information from multiple sources being provide to the operators. [Ref. 6:p. 1-1]

2. Navy Tactical Command System - Afloat (NTCS-A)

NTCS-A evolved from JOTS in the early 1990s, from the consolidation of a number of prototypes of individual "stovepipe" shipboard command and control software programs, including the Flag Data Display System (FDDS), the Joint Operations Tactical System (JOTS), the electronic Warfare Coordination Module (EWCM), and the Afloat Correlation System (ACS). [Ref. 3:p. 52] Additional NTCS-A functionality was incorporated from other stand-alone or prototype C4I systems such as the Prototype Ocean Surveillance Terminal (POST) and the Naval Intelligence Processing System (NIPS). Central to this consolidation effort was the abstraction of the afloat software into a common "core" set of software that could be used throughout the afloat community as the basis for their systems. This led to a set of common software originally called Government Off The Shelf (GOTS) version 1.1.

The common core software concept was extended to the shore community to

reduce development costs and ensure interoperability. This effort resulted in a collection of software commonly referred to as the Unified Build (UB) version 2.0 or GOTS 2.0. This software is now deployed both afloat, in NTCS-A, and ashore, in Operations Support System (OSS). The strength of these two systems is that they are built on top of a common set of functions so that advancements and improvements in one area are immediately translatable to advancements in the other area. [Ref. 6:p. 1-1]

3. Operations Support System (OSS)

OSS is a system that evolved from the functionalities of the Navy World-Wide Military Command and Control System (WWMCCS) Standard Software, Operations Support Group Prototype, Fleet Command Center Battle Management Program, and JOTS. This system is considered the shore installation variant of NTCS-A and is often referred to as Navy Command and Control System-Ashore (NCCS-A). By migrating the OSS into the JMCIS architecture, the Navy is seeking management economies of scale and performance enhancements in OSS.

C. JMCIS

JMCIS represents the next logical step in the evolution of Navy C4I systems. The addition of functions to NTCS-A has led to the creation of a new version of that system, which has been designated the Joint Maritime Command Information System. [Ref. 3:p. 56] JMCIS is described as a "overarching architecture" that is still evolving as fleet operators refine C4I requirements and the functionality of other systems is migrated

to the JMCIS architecture. The JMCIS approach to adding new functionality instead of building new systems allows the Navy to benefit from a single-configuration management approach. The system software provides the basic function, such as display control, message traffic control, and specific applications for various classes of equipped ships. [Ref. 3:p. 52]

Programmatically, JMCIS has consolidated the functions of NTCS-A and its complimentary ashore program, the OSS. The two systems are expected to form a significant core of the ongoing development of DoD-wide C4I architectures, referred to as Global Command and Control System (GCCS), that will continue to consolidate the C4I initiatives of the individual services. [Ref. 3:p. 52]

1. Genesis and History

JMCIS is the current state of C4I technology initially envisioned in 1981 by Vice Admiral (Ret.) Jerry O. Tuttle as the future of command and control. The JMCIS idea was cultivated from efforts to evolve interoperable C3I systems that began in the mid 1980's with the development of the Joint Operational Tactical System (JOTS) Command and Control System. The system was also designed to operate on the Tactical Advanced Computing (TAC) family of computers, as non-proprietary, open architecture that could be easily transported to subsequent improved versions of the TAC. [Ref. 6:p. 1-3]

Under the direction of SPAWAR (PD-60), the core software GOTS 1.1 was compiled for use throughout the afloat community as the basis for all C3I systems. GOTS 2.0 was called the Unified Build (UB) 2.0 and was developed to include the ashore

community to further increase C3I system interoperability. The Unified Build is confirmation of Vice Admiral (Ret.) Tuttle's statement :

> The future of C4I ... will be built on a foundation of interoperability, open systems, and a common operating environment. 'Standardization' will be our battle cry. [Ref. 7]

2. System Migration

In November 1993, Assistant Secretary of Defense (ASD) for C4I, Mr. Emmett Paige, issued a memorandum requiring all DoD services to develop a detailed plan for migration of individual systems into a common C4I framework. All systems nominated for migration to a common framework were to be completed within three years. Those systems not designated by the respective service as a candidate for migration were to either cease to exist or apply for exception status. [Ref. 8] Rear Admiral John Gauss of SPAWAR PD-60 stated that obsolete systems must be retired as soon as possible even if some functions have not been replaced due to the significant decreases in DoD funding. [Ref. 9] The ASD memorandum brought the issue of a common C4I framework espoused in the C4I For the Warrior plan to the front. A form of this common C4I framework was in existence prior to the issuance of the memorandum and JMCIS is that architecture selected for the U.S Navy and Marine Corps. Secretary Paige's memorandum accelerated existing Navy and Marine Corps migration planning and established JMCIS as a practical alternative for the other services. The legacy systems that were migrated into JOTS and eventually into JMCIS are depicted in Figure 3-1 [Ref. 10]. The systems that were initially migrated into JMCIS were operationally oriented and eventually this migration

philosophy was extended to logistical and intelligence related systems. Table 3-1 provides a listing of the full names for ... migrated systems.

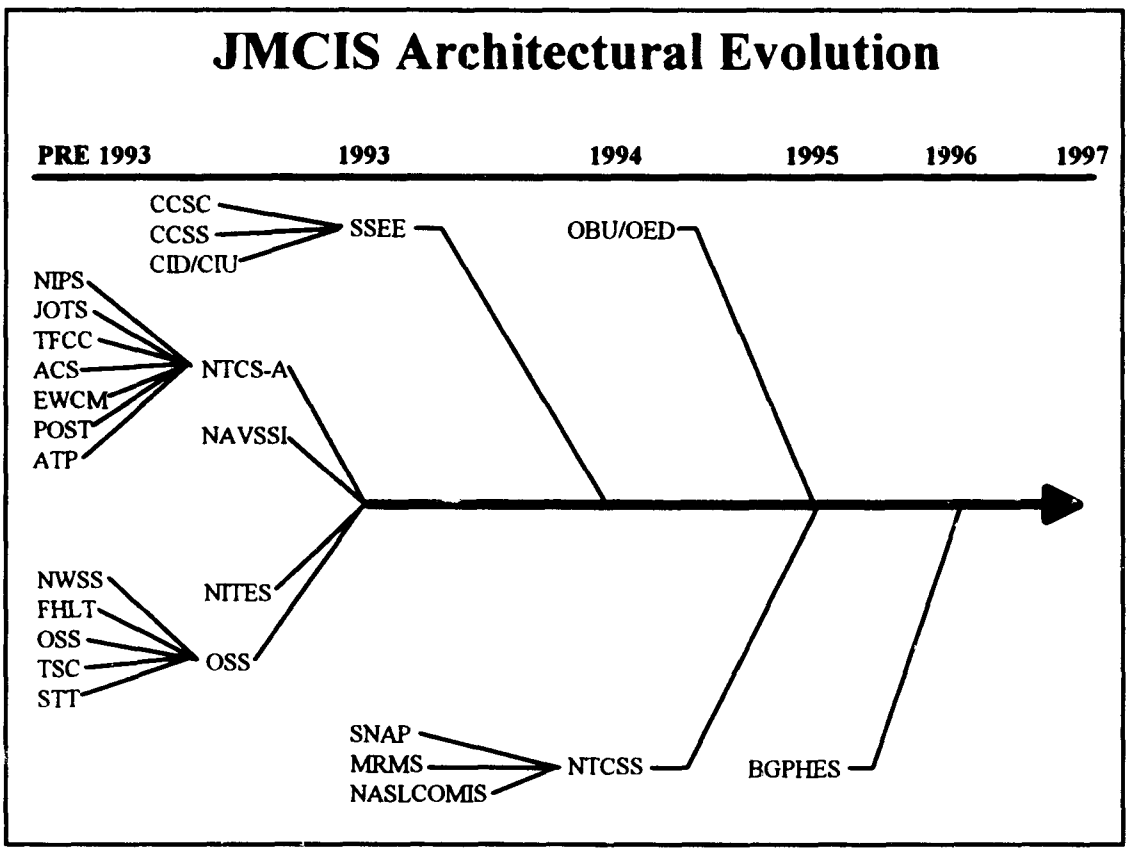

Figure 3-1 Migration of Legacy Systems [Ref. 10]

3. What is JMCIS?

JMCIS is a system built as an architectural framework to meet specific Navy and DoD command and control capabilities. Just like Microsoft Windows™, JMCIS provides an environment for applications that consolidates common functions. In Windows™, multiple applications can share common utilities such as printing and file

TABLE 3-1 MIGRATION SYSTEMS

Abbreviation	Full System Name
NIPS	NTCS-A Intelligence Processing Services
JOTS	Joint Operational Tactical System
TFCC	Tactical Flag Command Center
ACS	Afloat Correlation System
EWCM	Electronic Warfare Coordination Module
POST	Prototype Ocean Surveillance Terminal
ATP	Advanced Tracking Prototype
NWESS	Navy WMCCS Software Standardization
FHLT	Force High Level System
OSS	Operations Support System
TSC	Tactical Support Center
STT	Shore Targeting System
CCSC	Cryptologic Combat Support Console
CCSS	Cryptologic Combat Support System
CID/CIU	Cryptologic Interface Device/Unit
NTCS-A	Navy Tactical Command System - Afloat
NAVSSI	Navigation Sensor System Interface
NITES	NTCS-A Integrated Tactical Environmental Subsystem
SSEE	Ships Signal Exploitation Equipment
SNAP	Shipboard Non-tactical ADP Program
MRMS	Maintenance Resource Management System
NALCOMIS	Navy Aviation Logistics Command Management Information System
NTCSS	Navy Tactical Command Support System
BGPHES	Battle Group Passive Horizon Extension System
OBU/OED	Ocean Surveillance Information System (OSIS) Baseline Upgrade

management, rather than duplicating those functions for each application. For command and control systems, JMCIS provides various common utilities including mapping, tactical database display, and cartographic functions among others. This collection of utilities

comprises the JMCIS core and is graphically depicted as a part of the COE in Figure 3-2. [Ref. 6:p. 2-2] The core is maintained and expanded based upon the migration of legacy systems and improvements to existing JMCIS applications.

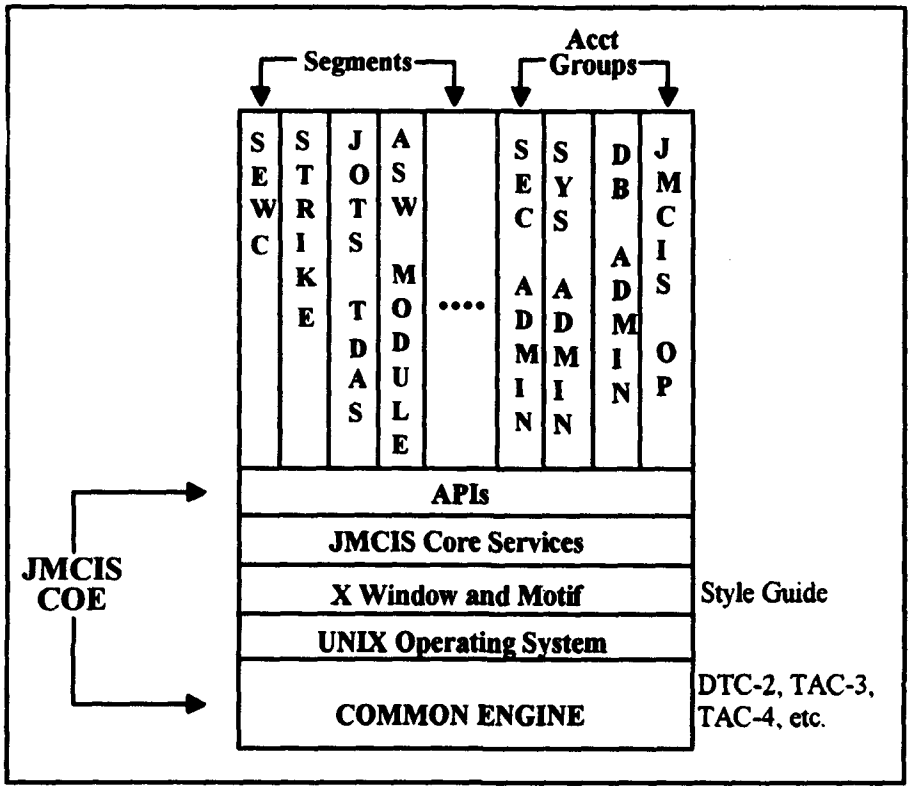

Figure 3-2 JMCIS COE [Ref. 6:p. 2-2]

The consolidation of common functions allows all applications to access the most efficient utility and provides the opportunity to easily update the core utilities with improved versions. In conventional client/server style, JMCIS servers provide core services to the rest of the LAN and each workstation may have both the same or different application software running.

a. Components of JMCIS

(1) Applications

Depicted vertically in Figure 3-2, applications access the JMCIS core services via Application Program Interfaces (APIs). In Figure 3-2 the applications annotated as 'Account Groups' are the standard applications that come as a part of JMCIS. These house-keeping applications are custom environments for the common activities of System Administration, Security Administration, Database Administration and the standard JMCIS operator environment. The applications annotated as 'Segments' are a sample of some of the unique applications that have been developed or migrated into the JMCIS environment. The specific Segments listed represent:

- SEWC - Space and Electronic Warfare Commander
- STRIKE - Strike Plot
- JOTS TDAS - Joint Operational Tactical System Tactical Decision Aids

(2) Common Operating Environment (COE)

The COE consists of the UNIX Operating System (OS), X Window graphical windowing system, and Motif standard styles, as well as core software for receiving and processing messages, correlation, updating the track database, and software for generating cartographic displays. [Ref. 6:p. 2-1]

(3) Unified Build (UB)

The UB is the foundation for all JMCIS software. The UB is a set of software components that include the Common Operating Environment (COE) and a

standard software base for central applications and library functions necessary for basic command, control, and supporting functions.

(4) Segment

A segment is a software application that operates in the JMCIS runtime environment utilizing core functionalities for common operations. Segments access the core functionality through a standard set of APIs. The standard set of APIs are managed by the core developers and are the access vehicle to core functionality. Unique functionality for individual segments is provided by the individual applications source executable code.

(5) Variant

A variant is a subset of segments, from the JMCIS Superset, installed for a specific mission area such as mission planning or battle group database management. The collection of various JMCIS segments are simply customized modules that define the JMCIS variant.

(6) GENSER Local Area Network / SCI Local Area Network

In most JMCIS applications there are two separate and distinct operational local area networks, referred to as JMCIS LANs. The GENSER local area network generates the primary tactical picture (situational display) and provides input to both the supported commander and also to the SCI local area network. The SCI local area network receives the GENSER information and applies SCI information, enhancing the GENSER picture. Downgraded or sanitized SCI information can also be provided

directly, via sanitization (Esprit/Radiant Mercury) to GENSER systems. [Ref. 11:p. 2] SCI and GENSER will be explained in more detail in Chapter III.

b. The Three Perspectives of JMCIS

(1) Sailor / Soldier Perspective

To the end user, JMCIS represents a Command Information System which is distributed across a Local Area Network (LAN) of workstations. Operators are able to access all required functionality from any workstation regardless of physical location or the actual location where the processing is taking place. The user is presented with only the functionality needed to meet their mission and other unneeded functionality is hidden to prevent overwhelming the user. An operator with a different set of tasks is presented with a different set of functionality but both operators perceive that the system looks and operates in the same way. JMCIS will appear to the operators as the identical Command Information System in use by military personnel in sister services with completely different mission objectives. This joint commonality is of increasing importance as a result of the expanded role the services are performing in the joint arena. [Ref. 6:p. 1-7]

(2) Program Manager Perspective

From the perspective of a military program manager, JMCIS presents the opportunity for an umbrella program which can encompass several programs. Faced with decreased funding, program managers can maintain program viability and achieve considerable savings by constructing their system from the JMCIS building blocks. In

these times of budget austerity, this potential savings is sometimes the only feasible option for the programs. [Ref. 6:p. 1-7]

(3) System Developer Perspective

From the perspective of a system developer, JMCIS is an open architecture and a software development environment that offers a collection of services and already-built modules for Command Information Systems. The JMCIS developers provide detailed instructions on how to make applications or systems JMCIS compliant. These instructions include details on standard user interface and the procedures for using core functionality via APIs. This core functionality has been previously developed and tested and therefore the developer need only produce components that are unique to their particular application. [Ref. 6:p. 1-7]

D. WHY JMCIS?

The evolution to JMCIS was an operational and financial necessity in today's world of rapidly changing technology and decreased funding for DoD systems. JMCIS provides DoD with an opportunity to stay ahead of technological growth well into the next century by implementing open systems architectures and ensuring standardization of software and hardware for C4I systems throughout the services.

1. Operational Justification

a. Command, Control, Communications, Computers, and Intelligence (C4I)

Command, control, communications and intelligence are pivotal to the success of any military mission. The addition of computers to the equation increases the fusion capabilities. The concept of computers being a force multiplier is espoused in the 1993 C4I For The Warrior document.

> Fused information is more valuable to the Warrior than information received directly from separate, multiple sources to the degree that it provides the warrior with 'real truth.' [Ref. 2:p. 13]

More importantly, the ability to pull on demand, information from any location at any moment, gives the Warrior both more flexibility and the skill to tailor decisions to his specific needs. [Ref. 2:p. 13]

b. Technology Explosion

Technological leaps are being experienced on an almost exponential scale. Rear Admiral Walter Davis, Head of the Warfare Architecture and Systems Engineering Directorate at the Space and Naval Warfare Systems Command (SPAWAR) summed up the speed of the development of technology by saying that "...the commercial computer industry is introducing new systems and new capabilities approximately every 18 months." [Ref. 3:p. 49-56] With the average DoD major automated information system (AIS) acquisition taking over 24 months from requirements specification to system delivery,

DoD is constantly being equipped with obsolete systems. *Open systems architecture is the solution.* The crux of open systems are common development standards from which products can be developed using non-proprietary specifications. The advantages of using open systems architecture to an organization the size of DoD are profound and present the most efficient and practical approach to the use of hardware and software.

One of the objectives of JMCIS is to avoid having command and control systems tied to a specific hardware platform or proprietary system. For this reason the JMCIS system is designed to operate on the family of TAC computers. The system is designed to be easily transported from one version of TAC computer to the next and be capable of exploiting the improved capability of the upgraded system. Rear Admiral Gauss stated that TAC hardware, COTS and GOTS software, and both government and industry standards, were to be used for all current and future JMCIS development. [Ref. 9] With the open architecture and commercial standards used by JMCIS, advances in computing platforms can be easily incorporated by simply changing the host machine for the system. Figure 3-3 presents the dramatic increase in the number of MIPS between successive TAC system procurements and the TAC-4 proposed processing capability of the TAC-4. [Ref. 7 and Ref. 12]

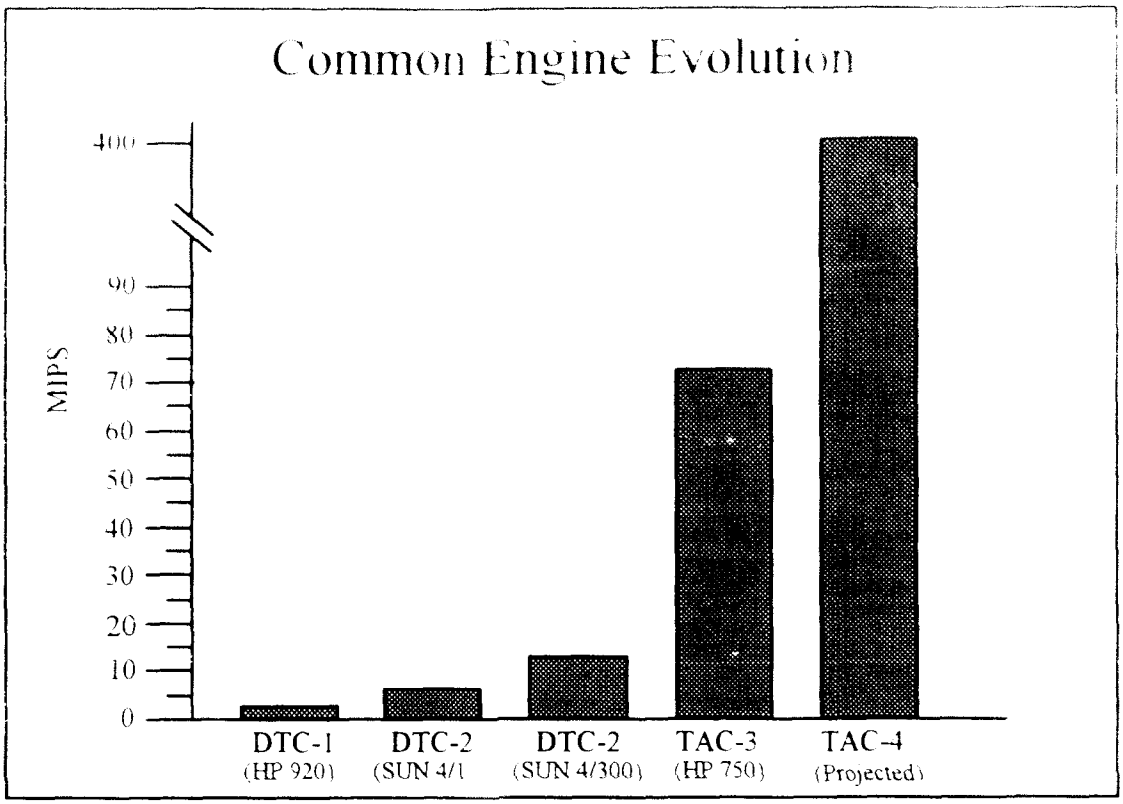

Figure 3-3 Platform Performance Improvements [Ref. 7 and Ref. 12]

c. Shared Access to Common Data

The Track Database is possibly the most important piece of the JMCIS Command Information System. This TDBM, coupled with the extensive communications capabilities of JMCIS, fosters greater interoperability with external sources and databases. The TDBM provides standard procedures and formats to add, delete, modify, and merge basic track data among the various workstations on the local area networks. With the increased capabilities of the TDBM to receive multiple sources of data, fusion of the information gives the warrior more intelligent correlation. [Ref. 6:p. 2-20]

Significant savings can be obtained by supporting a reduced number of lines of code. This reduction in lines of code is accomplished by implementing a common core of software and only producing the unique portions of the segment. Initial analysis of candidate command and control systems eligible for migration to JMCIS revealed significant reductions in post deployment software support.

a. Configuration Management - Hardware/Software

The financial savings of moving toward an open architecture environment cannot afford to be overlooked. While hardware costs have experienced a steady downward trend over the last several years, costs for proprietary software have mushroomed. The use of COTS software products combats the problem of skyrocketing costs by allowing the developer of a product to spread the cost of development among all users of the product. Achieving these economies of scale is the major cost saving characteristic of the JMCIS open architecture environment. Vice Admiral (Ret.) Tuttle noted that "... the expenditures on (software) applications -- coding, debugging, and testing -- spiral upwards to 90% of the total computer budgets." [Ref. 7]

b. Training

In addition to the costs for hardware and software, the costs related to training are significant. Through the use of open architecture and standardization of human machine interfaces, both operator and maintenance personnel familiarization with one system will translate directly to other systems using TAC hardware and open architecture environments. The Common Operating Environment (COE) of JMCIS

architecture environments. The Common Operating Environment (COE) of JMCIS includes such standards as X Window and MOTIF style guide as well as the UNIX operating system. By training operators on these standard vendor products, the familiarization time for new personnel is limited to the minimum necessary to understand the new mission and results in more rapid improvement in operator performance.

E. THE JMCIS PHILOSOPHY

1. Don't Reinvent the Wheel

If a component already exists, it should be utilized even if the component is not the optimum, best possible solution. As early as 1987 a GAO report on the issue of interoperability among DoD C3I systems noted that:

> Solving this problem (*of interoperability*) is no easy task. ... It will require a great deal of cooperation among the services and a genuine willingness on the part of each service to accept interoperability even when it conflicts with some traditional service practices. [Ref. 13:p. 18]

Almost any module can be improved but that is rarely the issue. For example, it is usually possible to obtain performance improvements in drawing speeds for cartographic displays by customizing designs to use hardware specific features. However, this may not be cost effective if platform portability is a requirement, or if performance gains are modest relative to perceived performance. [Ref. 6:p. 1-11] In addition, bottlenecks in the system often can't be determined until implementation and they often show up where they might not normally be expected.

2. Existing Standards

The commercial marketplace generally moves at a faster pace than the military marketplace and advancements are usually available at a faster rate. Use of commercial products has the advantage of lowering cost by using already built items, increases the probability of product enhancements because the marketplace is larger, and increases the probability of standardization. [Ref. 6:p. 1-12]

3. Interpretability

Interpretation of standards are a major source of problems with interoperability. To combat the problem, software modules should be reused across similar applications to decrease the likelihood of transference between entities. This ensures that the same standards are applied to all users and therefore eliminates the opportunity for inaccurate or varying interpretations. [Ref. 6:p. 1-12]

4. Focus Attention

Focus efforts on the development of desired but currently unavailable functionality instead of re-generating existing capabilities. [Ref. 6:p. 1-12]

F. THE OBJECTIVES OF JMCIS

Given the philosophy and history of the JMCIS concept, there are a number of objectives which are immediately apparent. The objectives include technical considerations such as software reusability, enforcement of common "look and feel", and

standardization of interfaces. These technical objectives in turn result in the potential for significant cost savings and development acceleration.

1. Commonality

Develop a common core of software that will form the foundation for Navy and Joint systems.

2. Reusability

Develop a common core of software that is highly reusable to leverage the investment already made in software development.

3. Standardization

Reduce program development costs through objectives one and two and through adherence to industry standards. This includes the use of commercially available software components whenever possible.

4. Engineering Base

Through standardization and an open JMCIS architecture, establish a large base of trained software/systems engineers.

5. Training

Reduce operator training costs through enforcement of a uniform human-machine interface, commonality of training documentation, and a consistent "look and feel."

6. Interoperability

Solve the interoperability problem (at least partially) through common software and consistent system operation.

7. Certification

Provide a base of certified software so that systems performing identical functions will give identical answers.

8. Testing

Increase the amount of common, reusable software to reduce testing costs because common software can be tested and validated once and then applied to many programs. [Ref. 6:p. 1-13]

G. THE FUTURE

The vision provided by strategic planning initiatives is being realized under the JMCIS banner. Systems continue to evolve toward the goal of an interoperable C4I system that focuses on support to the Warrior. The National Military Strategy Document (NMSD) for FY 1994-1999 establishes C4I as the overarching C4 programming objective and states that :

> Consistent with the C4I for the Warrior' plan, all Service and Agency programmed systems must be compatible and interoperable to support joint and combined operation across the entire spectrum of conflict. [Ref. 14]

GCCS is a Joint Staff sponsored program envisioned by the C4I for the Warrior concept and represents the next step in the evolution of command and control systems.

When fully implemented, GCCS will embody a network of systems providing the Warrior with a full complement of command and control capabilities. As part of the C4I for the Warrior concept, GCCS is evolving into the global, seamless "Infosphere" capable of meeting the Warrior's fused information requirements. [Ref. 2:p. 13]

III. THE SENSITIVE COMPARTMENTED INFORMATION (SCI) LOCAL AREA NETWORK

To understand the requirement for separate local area networks for General Service (GENSER) information and Sensitive Compartmented Information (SCI), an appreciation of Sensitive Compartmented Information as a separate classification category from GENSER is necessary.

A. SENSITIVE COMPARTMENTED INFORMATION (SCI)

SCI embodies a group of security clearances and compartments which require separate and more restrictive access and handling procedures than required of GENSER information. SCI is formally defined as follows:

> Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established. [Ref. 15:p. B-7]

The major distinction between SCI and GENSER information is the sensitivity of the information source. SCI information is afforded the highest conceivable security safeguards because the information collected or produced by certain SCI collectors is so sensitive that the possibility of compromising the source could have serious consequences. That is, if it was discovered that information was being collected from a specific source, that source could be eliminated or even worse, could be used as a funnel for

disinformation. In an SCI environment, averting the compromise of information is of paramount importance. [Ref. 16:p. 15]

Because SCI information requires separate handling and control procedures, the installation of equipment that processes SCI information is accomplished in separate and distinct spaces, both aboard ship and ashore. These special spaces, called "restricted" zones, "exclusion" zones, or Sensitive Compartmented Information Facilities (SCIFs) require that only those individuals who are appropriately cleared, and have specific need-to-know are given access. Further validation of the necessity for a separate local area network is given by:

> While the security afforded SCI data is sufficient for GENSER data, the reverse is not true. Thus, for example, a database in an SCI-accredited system could contain both GENSER and SCI information, but a GENSER database can contain only GENSER data. [Ref. 16:p. 8]

B. SCI LOCAL AREA NETWORK DESCRIPTION

1. Purpose of SCI LAN

The JMCIS SCI local area network supports all areas of command and control including situation status, planning, and execution of operations. Both organic (internal) and non-organic (external) sources of information are processed by the JMCIS local area networks. Assets of the supported commander provide the organic information which includes operations, surveillance, and intelligence data. Non-organic information is that data provided to the supported commander by external assets. [Ref. 17:p.2]

2. System Description

The GENSER local area network provides the primary tactical picture to the supported commander and also feeds the same information to the SCI local area network where it is fused with SCI information. This aggregate information, which provides a more complete overall picture can then be downgraded or sanitized and sent back to the GENSER local area network. The SCI local area network also provides SCI information directly to the supported commander as well as providing an SCI communications path for message release. [Ref. 11:p. 2]

The SCI local area network employs the system-high mode of network security. System-high basically means that everyone with access to the SCI local area network hold the security clearance and compartmentation approvals for all information processed on the network but may not have the need-to-know for all the information. There are different variants of the SCI local area network, but the standard objective architecture will include several Common Cryptologic Workstations (CCWS), Direction Finding (DF) Server Workstations, an Acquisition Server Workstation, and a Communications Workstation. Figure 3-1 illustrates the objective architecture of the SCI local area network and Table 3-1 defines the elements listed in the SCI LAN Objective Architecture.

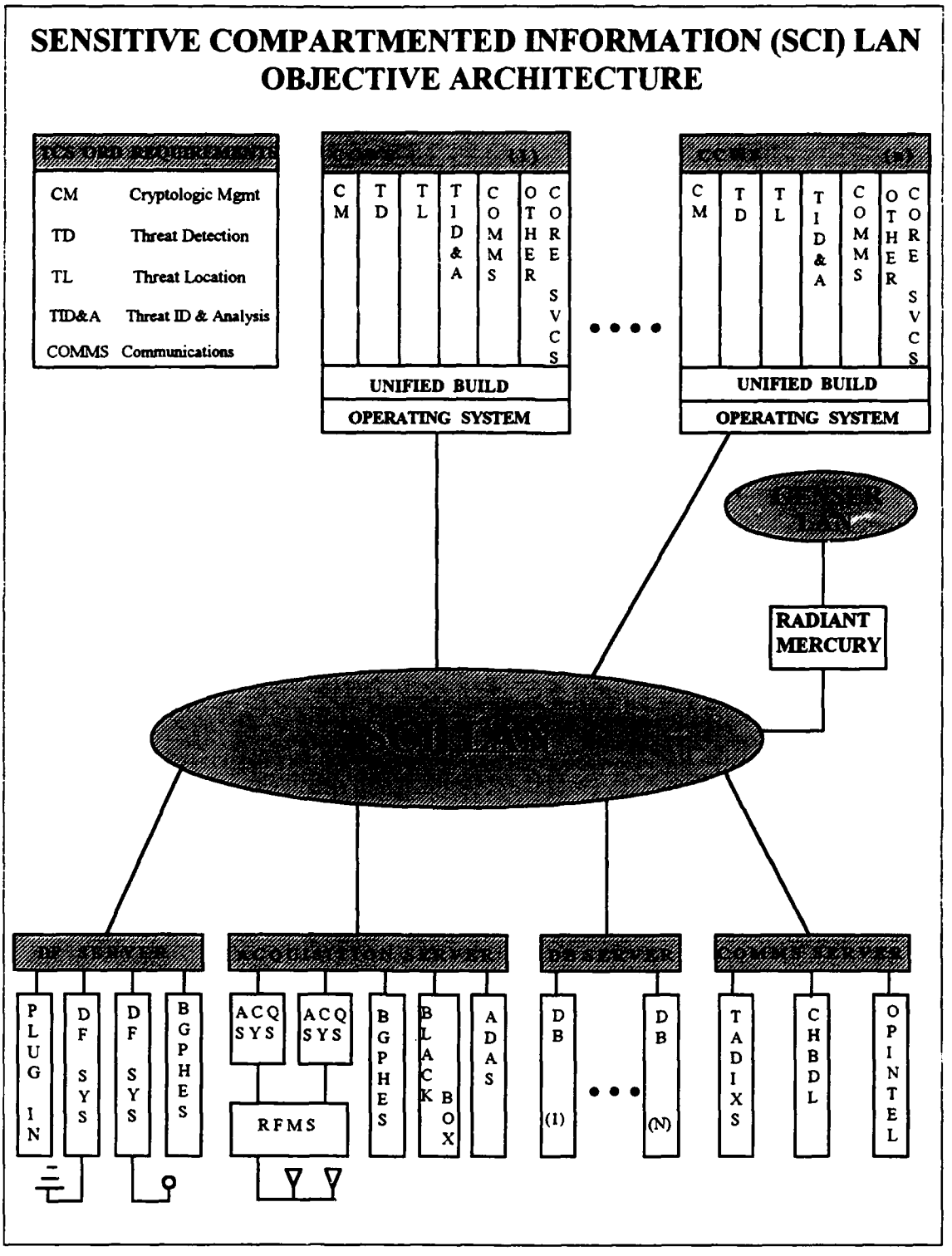

Figure 4-1 SCI LAN Objective Architecture [Ref 18:p. 6]

TABLE 3-1

Abbreviation	Full System Name
CCWS	Common Cryptologic Workstation
CM	Collection Management
COMMS	Communications
TD	Threat Detection
TL	Threat Location
TID&A	Threat ID and Analysis
DF Server	Direction Finding Server
DF Sys	Direction Finding System
BGPHES	Battle Group Passive Horizon Extension System
ACQ Sys	Acquisition System
RFMS	Radio Frequency Management System
ADAS	Automated Data Acquisition System
DB	DataBase
TADIXS	Tactical Data Information Exchange System
CHBDL	Common High Bandwidth Data Link
OPINTEL	Operational Intelligence

3. Unified Build

The foundation for JMCIS software is the Unified Build (UB). In addition to the Common Operating Environment (COE), the UB is a set of software components that include central applications and library functions necessary for basic command, control, and supporting functions. Some of the system data structures and functions included in the central applications include:

- System Administration
- Message Processing System
- File Manager

- CHART (maps)
- Tactical Display Manager [Ref 17:p. 5]

4. Segments

As previously described, a segment is a software application that uses JMCIS core functionalities for common operations. Segments access the core functionality through a standard set of APIs which are the access vehicle to core functionality. Unique functionality for individual segments is provided by each individual application. Specific segments on an SCI local area network are a function of the specific installation. That is, not all installations will have every segment installed since the mission and actual installation platform or site determine which segments are required. Current SCI local area network segments include:

- NTCS-A Intelligence Processing Services (NIPS)
- NTCS-A Imagery Exploitation Workstation (NIEWS)
- Strike Planning and Weapons System Support (STRIKE PLOT)
- Special Intelligence Correlator (SIC)
- Joint Deployable Intelligence Support System (JDISS)
- Collection Requirements Management Application (CRMA)
- Tactical Warning
- Analyst Workstation (AWS)
- Cryptologic Management [Ref 17:p. 6]

5. Security Functions

In the SCI environment the Security Manager can create, maintain, and delete user accounts as well as set audit parameters and retrieve audit trails. Privileged role (Security Manager, System Administrator, and Database Manager) actions are always audited and the audit trail cannot be edited. Auditing cannot be disabled on the SCI local area network and the LAN workstations and user classifications are always the same (system-high mode) and cannot be changed, even by the Security Manager. User access is limited to the tactical display windows and they cannot access the operating system or gain ROOT privileges. Root access can be established for system maintenance and all actions are audited. [Ref 17:p. 14]

To control access to the SCI local area network, both Role Based Access Control (RBAC) and Discretionary Access Control (DAC) are employed. Discretionary Access Control (DAC) will be explained in detail in Chapter IV and Role Based Access Control is simply another dimension to DAC. In this environment, the Security Manager assigns roles to individuals based upon their function and access is restricted based upon that function. To enforce individual need-to-know, DAC can be applied which can control individual access by allowing or disallowing execution of menu items from the function menus on the tactical display. [Ref. 17:p. 14]

IV. COMPUTER SECURITY

The issue of computer security is presented to both illustrate the vulnerabilities and threats to computer systems and introduce some terminology relevant to computer security. The significant increase in the use of computers throughout DoD, coupled with the rising number of reported computer system break-ins as a result of poor management practices and malicious intrusions, have given new impetus to the need for combating security related vulnerabilities. No where is this need more recognized than in the military and specifically in the arena of command, control and communications (C3). Interoperability among diverse C3 systems is being actively promoted as both a means of conserving DoD's scarce financial resources and also providing the capability for various systems and organizational units to share information. However, with this interoperability comes a host of security related problems. Most significantly, opportunities for malicious intruders to intentionally exploit weaknesses and subvert security control mechanisms are growing as a direct result of the interoperability brought about through the increasing use of open architecture environments. The Joint Maritime Command Information System (JMCIS), processing a wide range of classified material on the GENSER local area network and classified, compartmented information on the Sensitive Compartmented Information (SCI) local area network, is a prime target for exploitation by potential enemies.

A. WHAT IS COMPUTER SECURITY?

There are many definitions of computer security, but in the simplest terms, computer security refers to the protection of computer systems and the data associated with those systems against any deliberate or accidental compromise or unauthorized access through the use of technological safeguards and managerial procedures. Commonly called "information security" because of the information within a computer system, computer security consists of three characteristics: secrecy, integrity (or accuracy), and availability which are depicted in Figure 4-1. [Ref. 19:p. 4-6]

1. Secrecy

Secrecy refers to the ability of a computer system to allow only authorized users, by employment of a security clearance procedure, to access information within the system. Secrecy is the cornerstone of security in the JMCIS environment where multiple segments exist together on the local area network.

2. Integrity

Integrity is the ability of a computer system to ensure information within the system cannot be changed by unauthorized users and remains uncorrupted by the system itself. In the command and control arena, integrity is essential to the warfighter who depends on untainted data to make important theater battlefield decisions.

3. Availability

Authorized users should never be denied service. Availability is the capacity of a computer system to operate efficiently and fully recover following problems or system outages. In a military environment, availability equals dependability, and dependability is critical because time can be a major factor in a commander's decision making process.

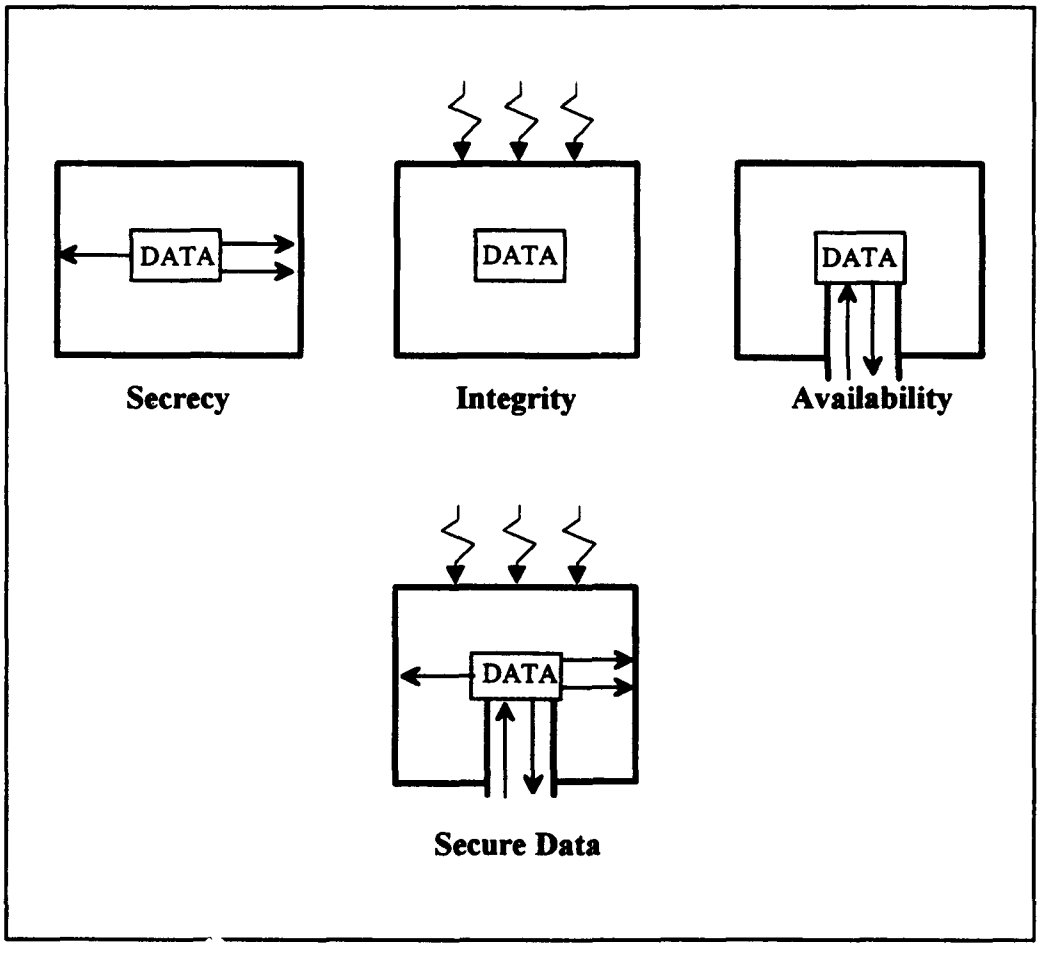

Figure 4-1 Characteristics of Computer Security [Ref. 19:p. 9]

B. WHY SECURITY?

In the context of command and control in general, and JMCIS in particular, the increasing demand and use of computers and local area networks has magnified the need for more emphasis on computer security. Over the last several years, numerous new computer systems have been implemented in the DoD that handle everything from accounting and logistic information to Top Secret Sensitive Compartmented Information (SCI). In a network environment, by simply logging into a terminal, a user may be able to access information from any machine attached to the network. The problem is obvious when viewed in relation to the range of classified and compartmented information processed on those systems.

Another issue of computer security is the effect of vulnerabilities introduced during software production. A significant quantity of commercial production software is produced in off-shore software development facilities, many of them in foreign countries not necessarily friendly to the United States. It is a relatively simple process for a programmer to introduce malicious code into software production and then make it appear as normal software code. These security threats, commonly called trap doors, Trojan horses, and viruses, can devastate a computer network and bring entire organizations dependent on those networks to their knees. A description of trap doors, Trojan horses, and viruses are provided in the glossary. Without strict controls on either how and where custom software is produced or on the procurement process of commercial software, serious consequences await. As the trend toward increased use of open systems

throughout DoD continues, aggressive attention must be given to the development and procurement of trusted products. One defense to malicious or corrupt software is the National Computer Security Center's (NCSC) "Trusted Product Evaluation Program" which assesses commercially developed software products to ensure availability of dependable off-the-shelf software for use by the U.S. government.

C. MODES OF SECURITY

There are three modes of operation for a computer network; dedicated, system-high, and multilevel, and each mode makes more refined distinctions among security parameters. That is, a dedicated mode network doesn't dependably distinguish between classifications or compartments, while a system-high network maintains separation of classifications solely by the need-to know parameters. Finally, a multilevel secure mode network should maintain divisions between need-to-know, compartments, as well as separation of data based on its classification. Each mode contains the characteristics of the previous mode and are thus successively more complicated and the risks of compromise is greater. [Ref. 20]

1. Dedicated Mode

Dedicated mode is when all users with access to a computer system or network meet the following criteria:

- possess a valid security clearance for **all** information processed on the system or any network attached to the system.

- have formal access approval (in addition to signed nondisclosure agreements) for **all** classified information (including **all** compartments) processed or stored.
- have a valid need-to-know for **all** classified information in the system. [Ref. 20]

2. System-High Mode

System-high mode is when all users with access to a computer system or network meet the following criteria:

- possess a valid security clearance for **all** information processed on the system or any network attached to the system.
- have formal access approval (in addition to signed nondisclosure agreements) for **all** classified information (including **all** compartments) processed or stored.
- have a valid need-to-know for **some** of the classified information in the system. [Ref. 20]

3. Multilevel Mode

Multilevel mode is when the following statements are satisfied with respect to the users with access to a computer system or network:

- some users **do not** have a valid security clearance for **all** the classified information processed on the system.
- all have the proper clearance and formal access approval for the classified information that they are to have access to.
- all have a valid need-to-know for the classified information that they are to have access to.

- Multilevel secure mode is not normally authorized for Sensitive Compartmented Information (SCI) applications. [Ref. 20]

The JMCIS SCI local area network operates in the system-high security mode. All personnel who have access to JMCIS SCI systems are cleared for the highest classification and compartmentation levels of information processed, although not all of those personnel have the need-to-know for all of the information.

D. EVALUATION CRITERIA FOR TRUSTED SYSTEMS

1. Background

The Department of Defense Trusted Computer System Evaluation Criteria (DoD TCSEC), called the "Orange Book", was created in 1985. The primary reason that the TCSEC was developed was the need to quantify trust or security in computer systems. Increasingly, government computer system procurements specify that computer technology meet the certification specifications of the TCSEC. The TCSEC has become the de facto standard for trusted systems. [Ref. 21:p. 104]

Trusted, in the context of computer security is synonymous with assurance and is simply the confidence in the ability of a computer system to measure up to its specifications. While a completely secure system is unattainable, some systems provide a higher degree of trust than others that they will correctly implement an access control policy. [Ref. 21:p. 105]

2. Purpose

The purpose of the criteria is to establish a set of measurable standards for evaluating the effectiveness of security controls built into computer systems by meeting three specific objectives:

- Give vendors of commercial computer products guidance and a benchmark for security features required to satisfy the trust requirements for sensitive applications.
- Provide a specific measure for the degree of trust that can be placed in a system that processes classified information.
- Establish a foundation for detailing security requirements in acquisitions specifications. [Ref. 22:p. 2]

3. Security Policy

A well-defined security policy is an essential requirement for achieving computer security. Simply put, a security policy is the rules that a computer system uses to determines whether or not access to the system will be granted. [Ref. 21:p.108] defines a security policy as:

> The set of rules and practices that regulate how an organization manages, protects and distributes sensitive information. It's the framework in which a system provides trust. A security policy is typically stated in terms of subjects and objects. A subject is something alive in the system; examples of subjects are users, processes, and programs. An object is something that a subject acts upon; examples of objects are files, directories, devices, sockets, and windows.

The TCSEC [Ref. 22:p. 3] states:

> There must be an explicit and well-defined security policy enforced by the system. Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object.

Fundamental requirements of a security policy are mandatory access control (MAC) and discretionary access control (DAC).

a. Discretionary Access Control (DAC)

In a system that processes classified information, discretionary access controls rules must be included in the security policy. "Discretionary security refers to a computer system's ability to control information on an individual basis." [Ref. 22:p. 75] When discretionary access control is implemented in a computer system, access to objects (files, directories, etc.) by subjects (users or groups) is restricted based upon the subjects identity and "need to know." The motive for discretionary security is that it allows the subject to decide on its own (discretion) what information under its control others subjects can access.

> Discretionary Access Control (DAC) is a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps) indirectly on to any other subject (unless restrained by mandatory access control). [Ref. 22:p. 112]

b. Mandatory Access Control (MAC)

Mandatory access controls must be included in the security policy of a computer system that processes classified information. In contrast to discretionary access

control, the computer system enforcing a mandatory access control policy removes the discretion and makes all decisions regarding what objects a subject can access. A mandatory access policy restricts access to objects by comparing a subject's security clearance level to the label (sensitivity of the information) of the object.

> Mandatory Access Control (MAC) is a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. security clearance) of subjects to access information of such sensitivity. [Ref. 22:p. 114]

4. The Criteria

There are four hierarchical divisions of security defined in the TCSEC; D, C, B, and A, with divisions C and B further divided into classes. The divisions and classes from the TCSEC are as follows:

a. Division D: Minimal Protection

Reserved for those systems that have been evaluated but fail to meet the requirements for a higher division.

b. Division C: Discretionary Protection

Provides discretionary (need-to-know) protection and accountability of subjects and actions.

(1) Class C1: Discretionary Security Protection

Provides for separation of users and data and sets controls for enforcing individual access limitations.

(2) Class C2: Controlled Access Protection

Provides finer granularity than C1 and makes users individually accountable through log-in procedures, auditing of security-relevant events, and resource isolation.

c. Division B: Mandatory Protection

Establishes the use of sensitivity labels to enforce mandatory access control rules. Also provides the security policy model on which the Trusted Computing Base (TCB) is founded and furnishes a specification of the TCB. Must also show that the reference monitor concept has been implemented.

(1) Class B1: Labeled Security Protection

Must provide an informal statement of the security policy model , data labeling, and mandatory access control over named subjects and objects.

(2) Class B2: Structured Protection

The Trusted Computing Base (TCB) is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in Class B1 systems to be extended to *all* subjects and objects. Covert channels are also addressed. Class B2 systems are *relatively* resistant to penetration.

(3) Class B3: Security Domains

Must mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To accomplish this, all code not necessary for security policy enforcement is excluded from the TCB. Class B3 systems are highly resistant to penetration.

d. Division A: Verified Protection

Characterized by the use of formal design specification and verification techniques to assure that the mandatory and discretionary security controls of the TCB can effectively protect classified information. Figure 4-2 shows how security increases as the divisions and classes progress and Figure 4-3 illustrates the specific attributes and requirements.

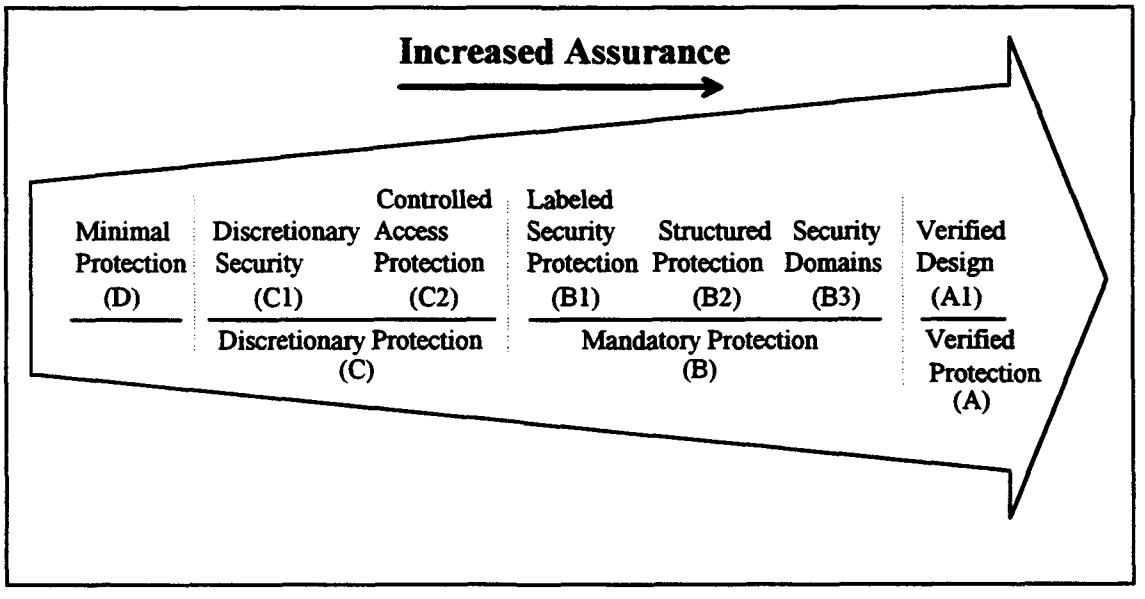

Figure 4-2 Trusted Computer System Rating Scale [Ref. 23:p. 68]

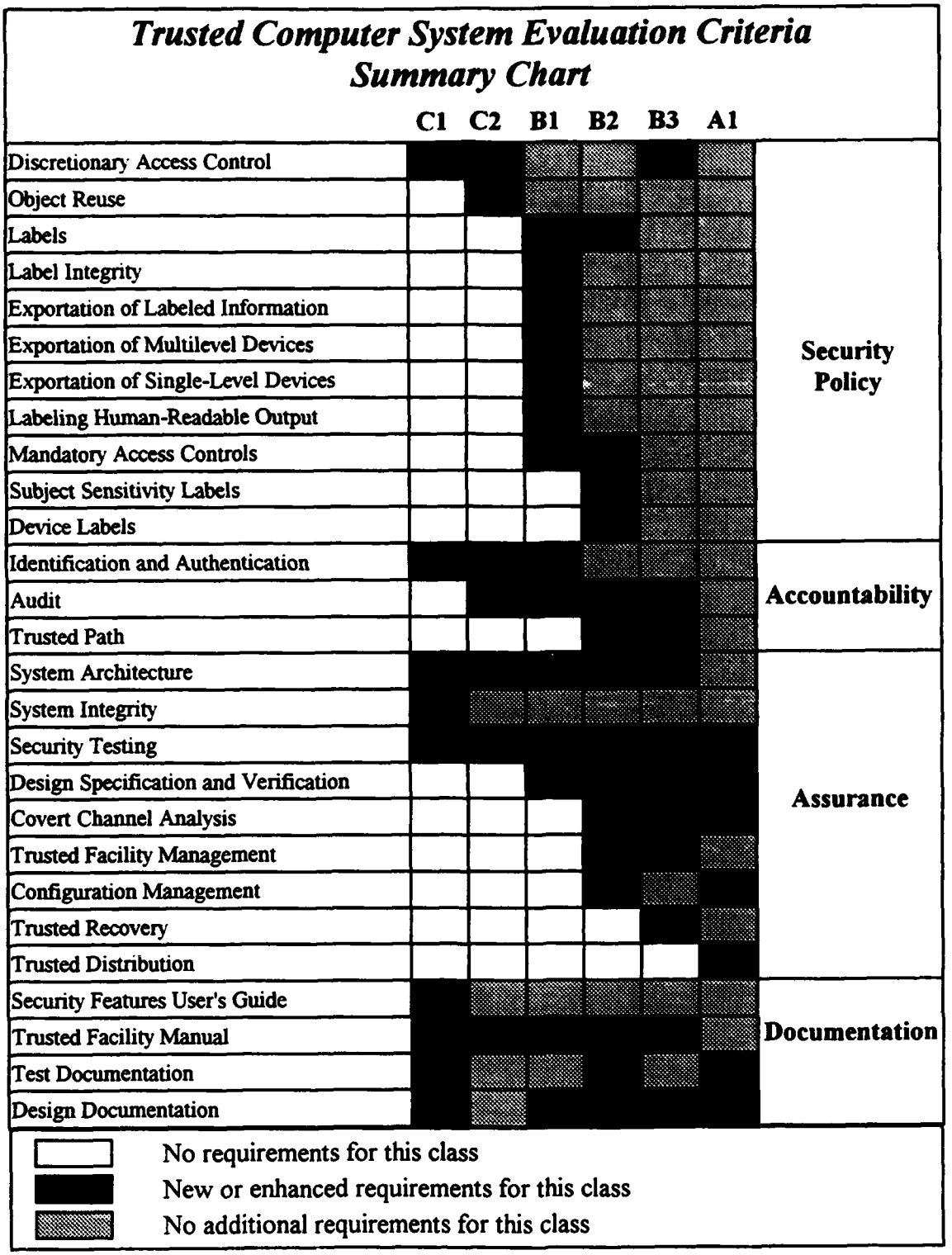

Figure 4-3 Comparison of Evaluation Classes [Ref. 22:p. 109]

E. COMMAND AND CONTROL SCENARIO

The means of exploiting computer systems require relatively moderate computer skills and vary widely from physical sabotage of equipment to deliberate penetration attempts. While deliberately far-fetched, the scenario that follows illustrates how the successful penetration of a command and control computer system can have devastating consequences. This scenario has been adapted from the original article, "The Importance of High Assurance Computers for Command, Control, Communications, and Intelligence Systems," [Ref. 24:p. 332-334]. Comparable articles can be found in [Ref. 25:p. 30-32] and [Ref. 26:p. 16]

> In 1995, the Department of Defense developed a project to interconnect various legacy command and control systems located throughout the world, at sea and ashore, with high speed, dedicated communications links. The preexisting systems had been in use for several years and were therefore considered secure as they each nominally enforced a mandatory security policy that provided adequate protection of classified information. For that reason, it was estimated that there was minimal additional risk to security produced by the new connectivity.
>
> In the subsequent conventional hostilities in the Middle East, this project was determined to be one of the decisive elements that led to the losses suffered by the NATO alliance. Unknown to the project developers, the enemy had successfully placed technical saboteurs at one of the ashore sites as early as 1989. That saboteur had managed to penetrate the system by installing a Trojan horse to exploit a flaw in the command and control system. By sending an illegitimate series of instructions (the Trojan horse) to an I/O device, an arbitrary memory location was modified and memory management access controls were circumvented.
>
> The Trojan horse, in the form of a virus infected graphics package, was obtained by a programmer working on the project from a public bulletin board system (BBS). Because the graphics package contained features that were needed for part of an application he was working on, the programmer loaded it into the command and control system for evaluation. After decomposing the graphics package, the

programmer decided it didn't satisfy the needs of the application and removed it from the command and control system. By this time though, the virus had become a permanent dweller in the command and control system.

In a targeted attack, the Trojan horse was purposefully located on the public BBS. Since the system programmers were known subscribers of the BBS, the chances of successfully penetrating the system were high. Also, because the BBS was open to the public, there was very little risk of apprehension for the saboteurs even if the Trojan horse was eventually discovered.

The Trojan horse had been engineered to exploit a specific defect on an identical computer system purchased off-the-shelf by the sabotage team in support of the attack. Included in the Trojan horse was the ability to accept covert software "upgrades" to its own program once it had installed itself. Thus, after the Trojan horse was installed, the saboteurs had complete access to the command and control system after communications with the Trojan were established. When the Trojan horse was initially activated, the first thing it did was notify the enemy operator as to its presence and location. It then relocated itself to the message processing subsystem where it could monitor all incoming message traffic. The Trojan horse also installed redundant processes in intelligent peripherals to watch for system maintenance and subsequent software upgrade installations, in effect assuring that the virus would remain in the system. The enemy then decided to forego use of the Trojan horse until it was militarily or diplomatically advantageous. So, for most of its life, the Trojan horse was inactive, and remained undetected.

Designed to communicate with the saboteurs via unclassified message traffic, the enemy could send and receive routine, unclassified, administrative messages and the DoD communication system would ensure delivery. By sending a preselected string of codewords and a "program" encoded as numeric table data, the enemy operator could signal and control execution of the Trojan horse. The enabling trigger and program code were designed to imitate a routine report originating from this and similar ashore sites, while ensuring that the risk of the "trigger" actually occurring in a genuine message was low. Similarly encoded signals from the Trojan horse could be sent to the enemy operator. To a cursory scan, the messages appeared to be routine logistics accounting messages containing tabular data.

With the interconnection of all command and control systems, the enemy could now subvert the entire U.S. command and control system network. After several years, the enemy successfully tested the Trojan horse to verify that it still existed and was operational. The Trojan horse was now reprogrammed to remotely access other

command and control systems and execute precise intelligence and disinformation tasks. They were now prepared to start the war.

The use of the Trojan horse during the war was done cautiously to avoid detection. The Trojan horse was used to determine allied order of battle information in addition to introducing small distortions to enemy track and locating data. These simple information modifications and alterations to system behavior were subtle enough to escape detection, but provided decisive intelligence and disinformation advantages, which are key ingredients to success on the battlefield.

V. SENSITIVE COMPARTMENTED INFORMATION (SCI) LAN SECURITY REQUIREMENTS

A. BACKGROUND

The security requirements for the JMCIS SCI local area network are derived from multiple sources, but primarily from the *Department of Defense Intelligence Information System (DoDIIS) Developer's Guide* which defines the fundamental security requirements and specific security modes of operation for SCI systems/networks. In addition, the *Trusted Computer System Evaluation Criteria (TCSEC)* is used to provide a general description of certain security requirements as listed in the *Concept of Operations and Security Analysis Guide* [Ref. 17].

B. PURPOSE

The purpose of this thesis is to provide an analysis for each of the specific security requirements under the broad category of Technical (Computer) Security. Communications Security (COMSEC) issues will not be discussed. The goal is to interpret the requirements and provide additional rationale for each specific requirement rather than critique whether the requirements have been met. The criteria established in the Trusted Computer System Evaluation Criteria (TCSEC), also called the "Orange Book"

or the "Criteria", and other relevant sources the author considers to be authoritative on the specific requirement will be used to provide the rationale for the analysis.

C. TECHNICAL (COMPUTER) SECURITY (TEC_1.0) REQUIREMENTS

1. Conceptual Design - TEC_1.1

a. Description

An engineering approach must be used to develop JMCIS 2.1 (SCI).

b. Interpretation and Rationale

This requirement is included to ensure that good engineering design and management practices are employed in the development of both the JMCIS SCI local area network Common Operating Environment (COE) as well as the individual application segments. Included in the requirement for "an engineering approach" are consistent software design methodologies and the acquisition of interoperable hardware. Additionally, configuration management procedures are employed to manage changes to the JMCIS SCI local area network. Configuration management refers to the methodical oversight of system modifications and ensuring that the modifications take place in an identifiable and controlled environment. Configuration management also ensures that changes are not detrimental to any properties of the system or affect the security policy. [Ref. 27:p. 3] Configuration management is defined as follows:

> The management of changes made to a system's hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the development and operational life of the system. [Ref. 27:p. 29]

2. System Architecture - TEC_1.2

a. Description

The Trusted Computing Base (TCB) must maintain a domain for its own execution that protects it from external interference or tampering.

b. Interpretation and Rationale

Prevention of modifications to the operating system code or data structures is the sum and substance of a trusted computer system. This requirement (TEC_1.2) specifies that the objects (files, directories, programs, displays, keyboards, printers, etc.) in the Trusted Computing Base be isolated from users and safeguarded against malicious threats and subversion. The TCSEC defines a Trusted Computing Base (TCB) as:

> The totality of protection mechanisms within a computer system--including hardware, firmware, and software--the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy. [Ref. 22:p. 116]

Since the JMCIS SCI local area network does not employ a trusted operating system at this time, the ability to meet this requirement (TEC_1.2) depends upon the basic security functions of the UNIX operating system, the hardware platform (DTC-2 or TAC-3), and the JMCIS Security Shell. The Security Shell prevents any user from having access to the operating system by restricting activity to general menu items and windows. The Security Manager specifies the level of access based upon the Account Group and

Role of the user, where the Account Groups permit access to specific applications and the Roles convey specific functionality within the applications. [Ref. 28:p. 21] Although the current mechanisms may help prevent accidental misuse, they do little to prevent direct probing, direct penetration, or subversion of the security mechanism. Figure 5-1 illustrates the Add Account Window used to enter new users into the system.

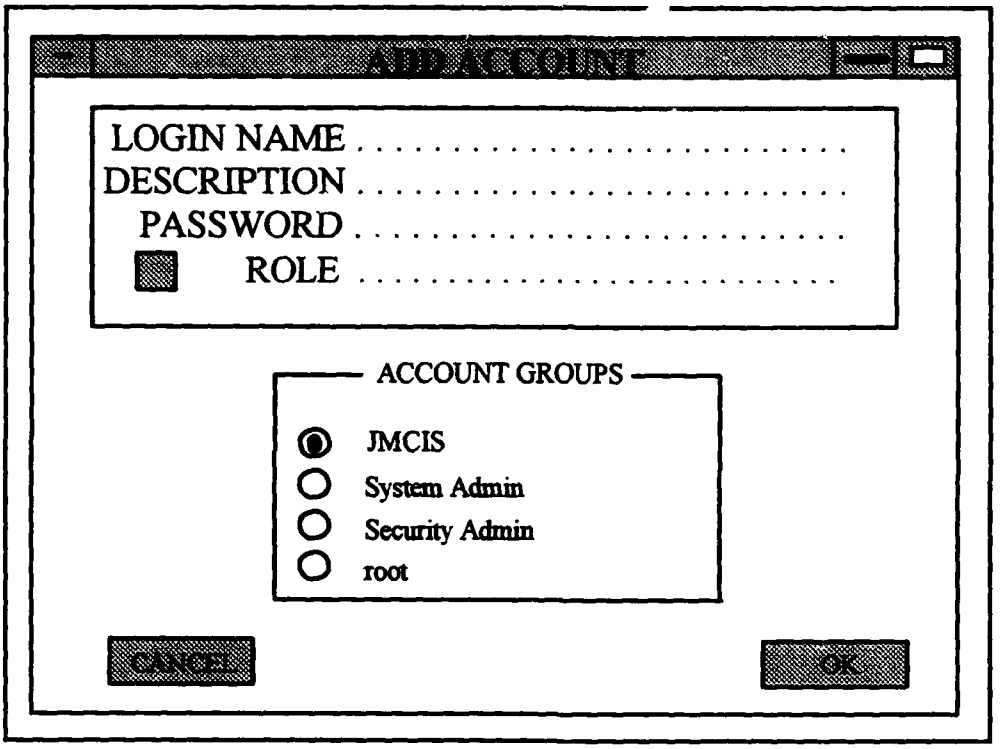

Figure 5-1 Add Account Window [Ref. 28:p. 21]

3. Discretionary Access Control - TEC_1.3

a. Description

JMCIS 2.1 (SCI) must enforce need-to-know.

b. Interpretation and Rationale

Limiting access predicated by the identity and need-to know of the user is called Discretionary Access Control (DAC). In a DAC environment, the user (subject) with permission to access specific objects may have the discretion to pass that permission to other subjects. [Ref. 29:p. 14] Discretionary control is the most common type of access control mechanism implemented in computer systems today. The discretionary security control objective is:

> Security policies defined for systems that are used to process classified or other sensitive information must include provisions for the enforcement of discretionary access control rules. That is, they must include a consistent set of rules for controlling and limiting access based on identified users who have been determined to have need-to-know for the information. [Ref. 30:p. 2]

SECNAVINST 5239.2 defines need-to-know as:

> A determination made in the interest of U.S. national security by the custodian of classified or sensitive unclassified information, that a prospective recipient has a requirement for access to, knowledge of, or possession of the information to perform official tasks or services. [Ref. 15]

Need-to-know in the SCI local area network environment is controlled by the Security Manager based upon a user's actual operational role to be performed. The Security Shell provides the functionality to control user access by role, granularity of access within a role, and information required to meet operational needs. [Ref. 17:p. 27] In this arrangement, a user may copy an object and pass it to another user, but access cannot be granted to others directly. This is called administratively controlled Discretionary Access Control.

4. Identification and Authentication - TEC_1.4

a. Description

Access must be controlled on the basis of unique User ID authenticated by password. For each AIS connected to the LAN, authentication data must be maintained and protected for every user.

b. Interpretation and Rationale

The process of identification and authentication begins with the login (identification) which establishes a communications path between the user and the system. After the communication path is set up, the user identifies himself (authentication). [Ref. 30:p. 4] Use of passwords is the most common form of authentication. For Class C2 level Controlled Access Protection the TCSEC states:

> The discretionary access control mechanism shall, either by explicit user action or default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users. [Ref. 22:p. 15]

and further:

> The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protection mechanism (e.g., passwords) to authenticate the user's identity. [Ref. 22:p. 16]

In the JMCIS SCI environment, as each new user account is created by the Security Manager, a unique User Identification and password is established. User Account information and authentication data is maintained in the *SECMAN* account which

is not accessible by users. Users can only perform functions defined for their respective roles.

5. Single User ID - TEC_1.4.1

a. Description

Each user must have a single, constant User ID regardless of logged on role.

b. Interpretation and Rationale

The audit requirement reinforces the demand for individual identity. This allows all users to be audited by the System Administrator based on their individual identity. The "Guide to Understanding Identification and Authentication in Trusted Systems" states:

> Identification and Authentication (I&A) must distinguish operators, system administrators, and system security officers from ordinary users in order to record security related events as actions initiated by the individuals performing those roles. Since individuals performing those roles may be ordinary users of the system, it is necessary to distinguish the people when acting as ordinary users. [Ref. 31:p. 13]

6. Password Length - TEC_1.4.2

a. Description

Minimum password length must be eight alphanumeric characters.

b. Interpretation and Rationale

A password should be difficult to predict, a mixture of alphabetic and numeric characters, upper and lower case, and at least eight characters long. Picking a password that meets these characteristics will decrease the chances of successfully

guessing by those with malicious intent. The Appendix provides a detailed explanation of the mathematics involved in establishing password length. [Ref. 32:p. 17]

7. Privileged User Limitation - TEC_1.5

a. Description

Number of logged on users must be limited to one privileged user per role at a time.

b. Interpretation and Rationale

This requirement has been modified by the Certification Authority in response to the operational need for multiple privileged users to be logged-on at the same time. For example, onboard ship, 24 hour a day operations are the norm and due to time constraints, two privileged users may be required to be working at the same time.

8. Role Change - TEC_1.6

a. Description

Role changes must be allowed "on the fly" (e.g., change user role without need to log off and log back on).

b. Interpretation and Rationale

This requirement doesn't apply to any specific threat or vulnerability. It is simply an efficiency measure to allow users with multiple role accounts to move back and forth between roles without being required to log out from one account and then log back in the other account. An example might be the Information System Security Officer

(ISSO) who is also an analyst. [Ref. 17:p. 28] In an open environment, using an untrusted path, if passwords are used to make the role changes, users could be spoofed and the passwords for privileged roles could be captured. Once JMCIS migrates to a trusted operating system, this will solve the issue for the GENSER local area network as well as provide further assurance for the SCI local area network.

9. Data Base Manager Role - TEC_1.7

a. Description

A Data Base Manager Role must be created to limit access to DBMS privileged functions.

b. Interpretation and Rationale

The integrity of the data in a Data Base Management System is the core of any system that permits users from different systems to share access to common data. In a command and control environment, where information is vital to significant decision making, data is a major asset and its consistency and integrity determine its value to the warfighter. The requirement for a Data Base Manager Role ensures controlled access to the database, which prevents unauthorized and untrained users to view data and decreases the chances of accidental or malicious modifications to the database.

10. Menu Item Gray-Out - TEC_1.8

a. Description

Menu items that are not valid selections for function being performed must be grayed-out or not displayed in menu.

b. Interpretation and Rationale

This requirement was created as a visual indication for individual users attempting to access menu items to which they are not authorized or cannot be executed for the specific function attempted. [Ref. 17:p. 29] This is somewhat analogous to the Data Base Management System (DBMS) projections in the Hinke-Schaefer architecture, that is, you don't see what you don't have access to and users don't even know that the field exists. [Ref. 33]

11. Audit - TEC_1.9

a. Description

An audit record must be maintained for AIS/network/user activity to permit regular or on-demand security reviews.

b. Interpretation and Rationale

The process of recording, inspecting, and evaluating any or all security-germane activities on a secure system is the process of auditing. The audit record is the primary means of monitoring user activity and piecing together the facts following a

security violation. The TCSEC defines an Audit Trail as:

A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions. [Ref. 22:p. 111]

The purpose of the Audit Mechanism is described as follows:

The audit mechanism of a computer system has five important security goals. First, the audit mechanism must "allow the **review** of patterns of access to individual objects, access histories of specific processes and individuals, and the use of the various protection mechanisms supported by the system and their effectiveness." Second, the audit mechanism must allow **discovery** of both users' and outsiders' repeated **attempts to bypass** the protection mechanisms. Third the audit mechanism must allow discovery of any **use of privileges** that may occur when a user assumes a functionality with privileges greater than his or her own, i.e., programmer to administrator. In this case there may be no bypass of security controls but nevertheless a violation is made possible. Fourth, the audit mechanism must act as a **deterrent** against perpetrators' habitual attempts to bypass the system protection mechanisms. However, to act as a deterrent, the perpetrator must be aware of the audit mechanism's existence and its active use to detect any attempts to bypass system protection mechanisms. The fifth goal of the audit protection mechanism is to supply "an additional form of **user assurance** that attempts to bypass the protection mechanisms are recorded and discovered." Even if the attempt to bypass the protection mechanism is successful, the audit trail will still provide assurance by its ability to aid in assessing the damage done by the violation, thus improving the system's ability to control the damage. [Ref. 34:p. 5]

12. Minimum Audit Data - TEC_1.9.1

a. Description

At a minimum, audit data must include User ID, Terminal ID, date, time, type of event, and success or failure of the event. Minimum audit events include: logon, logoff, application (menu item) access, file export to media or printer, file

creation/modification/deletion for user created /accessed files (e.g. messages), all actions by privileged users, STU-III (JDISS) time of call and external station's address.

b. Interpretation and Rationale

The minimum required audit data provides the auditor with the pertinent information necessary to reconstruct an event. Figure 5-2 illustrates the Security Audit Log which is created for each workstation on the SCI local area network. A similar log is created for auditing events in the operating system and is called the Operating System (OS) Audit Log.

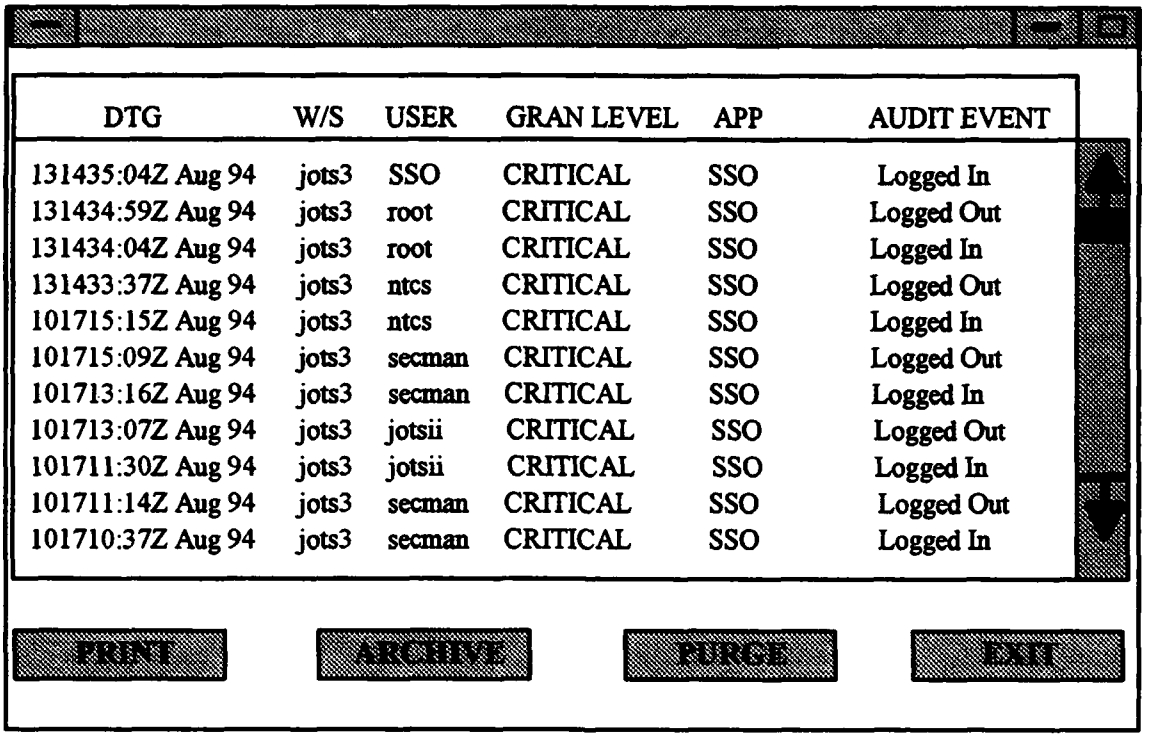

Figure 5-2 Security Audit Log [Ref. 28:p. 7]

13. Audit User Role - TEC_1.9.2

a. Description

The user role must be identified in audit records.

b. Interpretation and Rationale

Since users can have multiple roles within the JMCIS environment, it is necessary for the audit records to include information regarding the specific role a user is operating in to maintain a complete audit trail.

14. Audit Unsuccessful Log-on Attempts - TEC_1.9.3

a. Description

Each unsuccessful log-on attempt must be entered in the audit record.

b. Interpretation and Rationale

Auditing of unsuccessful logon attempts is important to determine malicious attempts to break in to the system. In addition, if users are notified of unsuccessful logon attempts with their own identification (ID), they can determine that another user has attempted to use their ID and the Security Manager can be notified. This might enable notification of malicious attempts to break in to the system prior to regular audit review. This requirement will not be fulfilled until the JMCIS SCI local area network migrates to a trusted operating system. [Ref. 17:p. 29]

15. Message Handling Audit - TEC_1.9.4

a. Description

JMCIS 2.1 (SCI) must maintain a record of all messages received and released.

b. Interpretation and Rationale

The ability to track incoming and outgoing messages is essential to maintaining a complete audit trail. The JMCIS SCI local area network records messages in several formats and include: Incoming Message Log (ILOG), the Incoming Message Catalog, the Outgoing Message Log (OLOG), and the Outgoing Message Catalog. These logs, when used in combination with the audit records, provide a thorough record of user activity. [Ref. 17:p. 29]

16. Log-on Alarm - TEC_1.10

a. Description

An alarm must be generated upon three successive unsuccessful log-on attempts. (Optimally, terminal locks with unlock possible only by security officer.)

b. Interpretation and Rationale

This requirement provides an audible alert that a user has unsuccessfully attempted to access the system and should be investigated. While the problem may be no more than simply typing in the authorized password incorrectly three times, it could also be an unauthorized user trying to logon or a user attempting to access an account or role

to which they are unauthorized. Standard Operating Procedures (SOPs) in most JMCIS SCI local area network installations apply the "Two-Man Rule", which means that two people are required in the facility or spaces at all times. The result is that all user activity is directly observable by at least one other user. In addition, in a System-High environment, unauthorized personnel are prevented from even accessing the spaces.

17. Marking Printed Output - TEC_1.11

a. Description

JMCIS 2.1 (SCI) must comply with appropriate directives for the mode of operation.

b. Interpretation and Rationale

This requirement is necessary to ensure that **all** material is printed with the proper classification level to prevent unauthorized disclosure and compromise of classified information. Human-readable sensitivity labels equal to at least the highest classification level and compartmentation will, **by default**, be placed at the top and bottom of each page of printed output to ensure that anyone viewing the material recognizes the classification level of the content. [Ref. 22:p. 22] Prior to release of printed material outside the JMCIS SCI System-High environment, the printed material is physically sanitized to the classification level at which it is being released. [Ref. 17:p. 30]

18. Object Reuse - TEC_1.12

a. Description

Authorization to information within a storage object must be revoked prior to initial assignment, allocation, or reallocation to a subject from the TCB's pool of unused storage objects. No information including encrypted representations, produced by a prior subject is to be available to any subject that obtains access to an object that has been released back to the system.

b. Interpretation and Rationale

Object reuse is a TCSEC Class C2 requirement and is defined by the *Guide to Understanding Data Remanence in Automated Information Systems* as:

> The reassignment to some subject of storage medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, no residual data can be available to the new subject through standard system mechanisms. [Ref. 35:p. 9]

This requirement simply means that a user who is issued memory space or storage should not have access to information previously placed in the storage location, regardless of whether the space was formerly allocated to another user or the current subject. The goal of Object Reuse is to prevent the leak of classified or sensitive information to untrusted users with access to storage objects in the JMCIS SCI local area network. While not protecting specifically against physical attacks on the system (e.g., using sophisticated equipment or software to recover residual information from memory or disk drives), Object Reuse prevents users (authorized and unauthorized) from browsing

or scavenging through the system looking for interesting items. The *Guide to Understanding Object Reuse in Trusted Systems* calls this the "equivalent of rummaging through the trash" [Ref. 36:p. 3].

19. Identification of User Terminal - TEC_1.13

a. Description

DCID 1/16 Requirement.

b. Interpretation and Rationale

This requirement follows the same reasoning as that from the previously discussed audit criteria. Identification of the specific user terminal in the audit data provides another piece of the required audit trail to track and reconstruct use of the system.

20. Automated Guard Processors and Filters - TEC_1.14

a. Description

Automated guards or filters must satisfy certain criteria for proper filtering of data streams.

b. Interpretation and Rationale

Before interpreting the requirement for Guard Processors and Filters, the distinction between the two should be made. The basic idea that follows, regarding Guards and Filters, is attributable to Dr. Roger Shell. A Filter simply looks at the data from a System-High environment to determine if it contains any of the classified words or

combinations of classified words, called "dirty words", in its reference database. If the data does contains any "dirty words", the filter sanitizes the data to a lower classification level and passes it on to a network of a lower level of classification. In the JMCIS environment the SCI local area network passes information to be transmitted to the Filter, in this case either the Esprit sanitizer or eventually, the Radiant Mercury interface. The information is then sanitized or downgraded and then passed on to the GENSER local area network. In the case of a Guard, the data is passed from one computer network to the guard, cryptosealed, and passed on to another secure computer network.

21. System Integrity - TEC_1.15

a. Description

Hardware or software features must be provided that can be used periodically to validate correct operation of hardware and firmware elements of the TCB. Features must be included that mandate loading of the security shell and prevents deactivation/deletion of shell.

b. Interpretation and Rationale

This feature is essential to ensure that the TCB is operating properly. Routine diagnostics are performed at system boot-up to test both hardware and software availability and operation. When the JMCIS SCI and Unified Build software is installed, the Security Shell is a mandatory installation item. On SCI local area network specifically, the workstation and user classifications remain at the network System-High classification level and cannot be changed, disabled, or deleted, even by the Security Manager.

[Ref. 28:p. 13] In addition to routine testing performed by the operating system, trusted recovery following system failure or emergency system shutdown is essential in restoring the system to a known trusted state.

22. Protection of Network Control - TEC_1.16

a. Description

The integrity of user identification and other security related information provided to remote hosts must be assured by appropriate means.

b. Interpretation and Rationale

This requirement ensures that both user specific information as well as security information reach the remote host in the same form as that transmitted without any degradation or corruption. The Transmission Control Protocol and Internet Protocol (TCP/IP), which provide for reliable data transfer and packet flow (checksums are used to check for damaged packets), are the standard protocols used in the JMCIS environment. Another view of this requirement comes from the term "trusted path", which expanded to encompass the path between distributed systems (remote hosts), simply means that the communications path is logically isolated and unmistakably distinguishable from other paths. [Ref. 22:p. 108] The article, "The Architecture of a Distributed Trusted Computing Base", contends that a trusted path offers the following guarantees:

a. A message received from a trusted path originates from a trusted source. This property can be supported in stronger form by authentication of the exact identity and security attributes of the originating component.

b. A message received from a trusted path contains the same value that was sent. This guarantees that message data have not been modified by untrusted entities.

c. If messages have security labels, then the label on a received message has the same value as that was sent. This guarantees that message labels have not been modified by untrusted entities.

d. An optional property is the preservation of message order on pairwise trusted paths. (This property also prevents replay of messages.) It is optional because it may be expensive to implement and difficult to verify. Further, it may not be required to support Trusted Computing Base (TCB) correctness. [Ref. 37:p. 70]

23. Integrity of Intelligence Data - TEC_1.17

a. Description

The network interface components must assure the integrity of intelligence they transmit.

b. Interpretation and Rationale

This requirement ensures that information is accurately transmitted from source to destination and is referred to as data integrity. The Transmission Control Protocol and Internet Protocol (TCP/IP), which provide for reliable data transfer and packet flow (checksums are used to check for damaged packets), are the standard protocols used in the JMCIS environment. There are various threats to communications integrity that include jamming/spoofing attacks, line and node outages, hardware and software failures, and actual active wiretapping attacks. To combat these threats, effective countermeasures must exist and that is the substance of this requirement (TEC_1.17). The countermeasures may include policy, procedures, automated or physical controls,

mechanisms, and various protocol means that ensure data has not been subject to excessive random errors and unauthorized message stream modification (MSM) such as alteration, substitution, reordering, replay, or insertion. The Trusted Network Interpretation (TNI) states:

> When ciphers are used in networks, it is combined with network protocols to protect against unauthorized data modification. The strength of the ciphers, the correctness of the protocol logic, and the adequacy of implementation are three primary factors in assessing the strength of Data Integrity using cryptography techniques. [Ref. 38:p. 182]

24. Security Markings For Exported Intelligence - TEC_1.18

a. Description

Every AIS must be able to provide, either explicitly or implicitly, security parameters for the intelligence it stores and processes. Such parameters must be reliably associated with other AISs.

b. Interpretation and Rationale

This requirement ensures that any information exported to other networks is of at least the same level of classification as the exporting system. This prevents unauthorized disclosures or compromises to systems and users not cleared for the level of information from the exporting system.

25. Security Testing - TEC_1.19

a. Description

TCSEC requirement covers testing of security mechanisms prior to certification of test.

b. Interpretation and Rationale

The TCSEC defines security testing as:

> A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process also includes hands-on functional testing, penetration testing, and verification. [Ref. 22:p. 115]

In accordance with good engineering practices, all security features including the Security Shell are rigorously tested to determine both functionality and ability to migrate to the JMCIS environment. Testing is done both during development by the developer and again at the Naval Research and Development (NRaD) facility in conjunction with integration to JMCIS. The *JMCIS SCI Concept of Operations and Security Analysis* document specifies that:

> A Security Certification Test, under the direction of the Certification Authority, of JMCIS 2.1 (SCI) will be performed in the NRaD System Integration Laboratory. The purpose of this test is twofold: 1, certification of JMCIS 2.1 (SCI) as installed for integration at NRaD; and 2, it serves as a pretest of the architecture, functionality, and security of JMCIS 2.1 (SCI) prior to its installation at operational locations. While the physical configuration is different, the system architecture, hardware components, and software in the integration laboratory is identical to that which will be installed at operational locations. [Ref. 17:p. 33]

26. Trusted Operating System - TEC_1.20

a. Description

Migrate to a Trusted Operating System for JMCIS SCI.

b. Interpretation and Rationale

Before discussing a Trusted Operating System, some background information is provided. The *reference monitor* concept was introduced to information system design to prevent unauthorized or inadvertent disclosure of information from one security level to another. The *reference monitor* concept is basically an abstract access mediation mechanism between subjects and objects that controls access by referencing an authorization database. The implementation of the reference monitor is called the *security kernel*. The *security kernel* and the operating system must be protected within the boundary of what is called the Trusted Computing Base (TCB). An operating system is called trusted when all operating system actions are properly mediated through the *security kernel*. The key reason for implementation of a Trusted Operating System is the necessity for guarding against malicious software as well as direct penetration attempts and other subversion threats. Implementing a Trusted Operating System is relevant because mediation of access between users and objects is essential in enforcing a unified security policy.

27. DoD Banner - TEC_1.21

a. Description

The DoD interest system banner must be presented to each user upon logon.

b. Interpretation and Rationale

This requirement was established as a visual indication to users that they are accessing a DoD computer system when they logon. This is just a simple reminder that enforces security at the conscious level and acts as a deterrent in warning users that all actions are monitored and audited.

28. Session Security Parameter - TEC_1.22

a. Description

A control feature, such as a security session parameter, must be provided for each exchange of intelligence by AISs, according to each of the four modes of operation.

b. Interpretation and Rationale

Since the JMCIS SCI local area network operates in the System-High mode, all exchanges of intelligence are treated as if they were at the highest classified, most sensitive level in the system. The System-High mode is when all users with access to a computer system or network meet the following criteria:

- possess a valid security clearance for **all** information processed on the system or any network attached to the system.

- have formal access approval (in addition to signed nondisclosure agreements) for **all** classified information (including **all** compartments) processed or stored.

- have a valid need-to-know for **some** of the classified information in the system.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The primary goal of this thesis was to analyze the various security requirements established for the Joint Maritime Command Information System (JMCIS) Sensitive Compartmented Information (SCI) local area network. While the security requirements for the JMCIS SCI local area network are derived primarily from the Department of Defense Intelligence Information System (DoDIIS) Developer's Guide, a different outlook was desired for this analysis. Therefore, to approach the security requirements from another perspective, the criteria set forth in the Trusted Computer Systems Evaluation Criteria (TCSEC) as well as other established and authoritative standards were employed to survey and describe the requirements. There are several broad areas of security in the JMCIS SCI local area network but this thesis examined the *Technical (Computer) Security Requirements* exclusively.

Another purpose of the thesis was to convey an awareness of the significant complexities involved in establishing security requirements in an environment designed to process Sensitive Compartmented Information (SCI). Foremost in the minds of those developing secure systems is the issue of adequate security protection. That is, is there a threat and if so, is the system adequately protected? If a system is developed completely in a trusted environment, the risk of subversion as a result of people with malicious intent

is reduced. In contrast, a system developed even partially in an untrusted environment can bring with it a much larger set of problems as seen in the command and control scenario described in Chapter IV. Many of the threats and vulnerabilities to computer system security are avoided in the SCI environment simply by making the security mode System-High. In a System-High environment, where all those with access hold a security clearance for **all** of the information processed in the system, physical access to both the spaces and the network itself by unauthorized personnel is prohibited. As a result, the risk of compromise or unauthorized disclosure is minimized considerably over that of the GENSER local area network where the environment is more open and limiting access is much more difficult.

Implementation of the System-High mode of security has its drawbacks as well. In this environment, computer security as enforced is inherent primarily in the architectural design of the facility rather than in hardware or software controls. As a result, it becomes easy to fall back on the notion that simply due to the System-High mode, security is more or less invoked as a matter of policy. Fortunately, in the design of the JMCIS SCI local area network, significant emphasis and forethought have been provided by the developers to secure a high level of assurance that system security will be enforced.

B. RECOMMENDATIONS

The results of the security requirements analysis of the JMCIS SCI local area network support the prerequisites for accreditation of an SCI system in a System-High environment. As the evolution of JMCIS proceeds into the Global Command and Control

System (GCCS), there are several deferred requirements that those concerned with the development of the Sensitive Compartmented Information (SCI) section of the architecture should remain cognizant of and push for compliance. A brief discussion of selected deferred requirements will follow with appropriate recommendations.

1. TEC_1.2 and TEC_1.20

The TEC_1.2 security requirement description is that the Trusted Computing Base (TCB) must maintain a domain for its own execution that protects it from external interference or tampering. The description of TEC_1.20 is to migrate to a Trusted Operating System for JMCIS SCI.

These two requirements are related in that they are both concerned with the TCB. The implementation of requirement TEC_1.20 would, by implication, fullfil the requirement of TEC_1.2. The key reason for implementation of a Trusted Operating System is the necessity for guarding against malicious software as well as direct penetration attempts and other subversion threats. Currently, the TCB consists only of the untrusted UNIX operating system security features and the SCI Security Shell. While the operating system security features and the SCI Security Shell may preclude accidental misuse, they don't provide much assurance against intentional subversion.

While the System-High security mode provides a physical security barrier, implementation of a Trusted Operating System would provide enforcement of the access control policy within the computer and thus more assurance that the system is subversion-resistant. Migration to a Trusted Operating System should remain a high

priority. It should be noted that because of the distributed nature of this system, the Trusted Network Interpretation (TNI) [Ref. 38] as well as the TCSEC will be applicable for an assessment of the security policy enforcement mechanism.

2. TEC_1.9.3 and TEC_1.10

TEC_1.9.3 requires that all unsuccessful logon attempts be entered in the audit record and TEC_1.10 requires that an alarm be generated after three unsuccessful logon attempts. These two requirements are discussed together because monitoring unsuccessful attempts to logon to the system is an essential security feature in a trusted system. TEC_1.9.3 and TEC_1.10 do not currently comply and are deferred until the SCI local area network migrates to a trusted operating system.

Auditing of unsuccessful logon attempts is essential in establishing a trail of records that aid monitoring user activity, especially following a security violation. The ability of a system to provide a complete audit trail is a significant deterrent to malicious probing. An audible alarm generated after unsuccessful logons is also a deterrent to malicious attempts to break-in to a system. In the SCI environment, most facilities require the "Two-Man Rule" which decreases the hazard of users attempting to logon to another account. Nevertheless, monitoring unsuccessful logons is an important aspect of computer security and these two requirements should be implemented as soon as possible.

3. TEC_1.12

TEC_1.12 concerns object reuse and is a fundamental TCSEC requirement for Class C2 systems.

Object reuse concerns information left in a memory storage location. The TCSEC requirement is that no user should have access to information previously put in a memory storage location. This is a significant requirement because it prevents users from having access to information for which they don't have formal clearance for or the appropriate need-to-know. Since this is another feature provided by the operating system, this requirement cannot be implemented until the SCI local area network migrates to a Trusted Operating System.

4. TEC_1.16

The TEC_1.16 requirement, Protection of Network Control, requires that the integrity of user identification and other security related information provided to remote hosts must be assured by appropriate means. Because the JMCIS SCI LAN is a network, concepts from the Trusted Network Interpretation (TNI) [Ref. 38] are applicable in order to provide a coherent level of assurance for the system. An analysis of the system from the distributed Trusted Computing Base (TCB) perspective will identify that a trusted path between distributed elements of the partitioned TCB is necessary. Communications Security (COMSEC) techniques may be appropriate to address this requirement.

The results of this thesis' analysis support the established security requirements in general, but the migration of the JMCIS SCI local area network to a Trusted Operating System should be a high priority.

APPENDIX

A. DETERMINING PASSWORD LENGTH

The security afforded by passwords is determined by the probability that a password can be guessed during its lifetime. The smaller that probability, the greater the security provided by the password. All else being equal, the longer the password, the greater the security it provides. This appendix reviews the mathematics involved in establishing how long a password should be.

The basic parameters that affect the length of the password needed to provide a given degree of security are:

L = maximum lifetime that a password can be used to log into the system.

P = probability that a password can be guessed within its lifetime, assuming continuous guesses for this period.

R = number of guesses per unit of time that it is possible to make.

S = password space, i.e., the total number of unique passwords that the password generation algorithm can generate.

1. Relationship

Considering only the cases where S is greater than L x R and therefore P is less

---

This entire Appendix was taken from Appendix C of the Password Management Guideline [Ref. 32:p. 17].

than 1, the relationship between these parameters is expressed by the equation:

$$P = \frac{LxR}{S}$$

2. Guess Rate

Several factors contribute to the rate at which attempts can be made to gain access to the data on a system when a valid password is not known. First and foremost is the protection given to the password database itself. If the password database is unprotected (i.e., can be read by anyone as ordinary data), then "guessing" may not be required.

If the password database can be read, but the passwords are encrypted, a very high guess rate may be possible by using a computer to try a dictionary of possible passwords to see if ciphertext can be generated that is the same as on in the password database. A similar situation frequently occurs where only passwords are used to protect files.

Finally, if the password database has effective access controls and the login procedure cannot be bypassed , the guess rate can be controlled by setting limits on the number of login or other attempts that can be made before terminating the connection or process.

3. Password Lifetime

All other things being equal, the shorter the lifetime of a password, the fewer the number of guesses that can be made and thus the greater the degree of password security. **The maximum password lifetime should not exceed one year.**

4. Password Space

Password length and alphabet size are factors in computing the maximum password space requirements. The following equation expresses the relationship between $S, A,$ and M where:

S = password space

A = number of alphabet symbols

M = password length

$$S = A^M$$

To illustrate: If passwords consisting of four digits using an alphabet of 10 digits (e.g., 0-9) are to be generated:

$$S = 10^4$$

That is, 10,000 unique 4-digit passwords could be generated. Likewise, to generate random 6-character passwords from an alphabet of 26 characters (e.g., A-Z):

$$S = 26^6$$

That is $3.089 * 10^8$ unique 6-character passwords could be generated.

"User friendly" passwords (sometimes referred to as passphrases) could be generated by using, for example, 3 symbols from an alphabet (dictionary) of 2000 symbols, where each symbol was a pronounceable word of 4, 5, or 6 characters. Using the previous equation and setting:

A = 2000 symbols (words)

M = 3

then $S = 2000^3$

That is, $8 * 10^9$ unique passwords could be generated where each password was made up of 3 words taken from a dictionary of 2000 words.

5. Procedure For Determining Password Length

What is important in using passwords is how long to make the password to resist exhaustive penetration attacks. There are several procedures for determining acceptable length as follows:

a. Establish an acceptable probability, P, that a password will be guessed during its lifetime. For example, when used as a login authenticator, the probability may be no more than 1 in 1,000,000. In another case, where very sensitive data is involved, the value for P may be set at 10^{-20}.

b. Solve for the size of the password space, S, with the equation $P = \frac{LxR}{S}$ where $S = \frac{G}{P}$ and $G = LxR$

c. Determine the length of the password, M, from the equation

$$M = \frac{\text{Log S}}{\log (\text{number of symbols in the "alphabet"})}$$

M will generally be a real number that must be rounded up or down to the nearest whole number.

6. Example of Password Length Determination

The problem is to determine the needed password length to reduce to an acceptable level the probability that a password will be guessed during its lifetime. The network to which this is applied supports a 300 baud service. Experiments on the

network have determined that it is possible to make about 8.5 guesses per minute. An arbitrary value of 10^{-6} is used for the probability, P, of guessing the password in its lifetime (as long as the password is changed at least once per year, the password lifetime is not a critical factor).

The statement of the problem is to find a password length that will resist being guessed with a probability of 1 in 10^6 in 1 year of continuous guesses. When three parameters in the following equation are known, the fourth value can be found: $P = \frac{LxR}{S}$. The following parameters are given:

L is set for 6 months and 12 months.

P is set for 1 in 1,000,000 (acceptable probability of guessing the password).

R is set at 8.5 guesses per minute.

At 8.5 guesses per minute, the number of guesses per day would be 12,240. Substituting 183 days for 6 months gives:

$$S = \frac{G}{P} = \frac{183 \times 12240}{.000001} = 2.23992 \times 10^{12} \text{ passwords}$$

The 12-month value is twice that of the 6-month case.

With this data and using the equation:

$$M = \frac{\text{Log } S}{\log (\text{number of symbols in the "alphabet"})}$$

the length of the passwords as a function of the size of the alphabet from which they are drawn can be determined. Assume two alphabet sizes; a 26-letter alphabet and a 36-letter-and-number alphabet.

$$M = \frac{\log (2.23992 \times 10^{12})}{\log 26} = 8.72 \text{ (for 6-month lifetime)}$$

$$M = \frac{\log (4.4676 \times 10^{12})}{\log 26} = 8.94 \text{ (for 12-month lifetime)}$$

$$M = \frac{\log (2.23992 \times 10^{12})}{\log 36} = 7.93 \text{ (for 6-month lifetime)}$$

$$M = \frac{\log (4.4676 \times 10^{12})}{\log 36} = 8.13 \text{ (for 12-month lifetime)}$$

Table 1 presents the results.

TABLE 1

MAXIMUM LIFETIME (months)	Length of Password	
	26-Character Alphabet	36-Character Alphabet
6	9 (rounded up from 8.72)	8 (rounded up from 7.93)
12	9 (rounded up from 8.94)	8 (rounded down from 8.13)

REFERENCES

1. Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, U.S. Department of Defense, *Corporate Information Management for the 21st Century, A DoD Strategic Plan*, June 1994.

2. C4 Architecture Integration Division (J6I) J6, The Joint Staff, *Committed, Focused, and Needed, C4I For The Warrior*, Government Printing Office, Washington, DC, 1993.

3. Walsh, Edward J., "Navy Aims at Joint Operations Roles and Economies for C4I," *Sea Power*, , April 1994

4. Copernicus Architecture, *Phase 1:Requirements Definition*, 1991.

5. Dearborn, Rebecca D., and Morales, Robert C., *An Overview of the Copernicus C4I Architecture*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1992.

6. Inter-National Research Institute, Inc., *Joint Maritime Command Information System (JMCIS) Common Operating Environment (COE)*, Rev 1.4, February 1994.

7. Tuttle, Jerry O., "OPNAV N6" brief presented to the JMCIS Joint Requirements Working Group (JRWG), Dam Neck, Virginia Beach, Virginia, 19 October 1993.

8. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, *Memorandum for Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, and Directors of the Defense Agencies regarding Selection of Migration Systems*, December 1993.

9. Gauss, John A, RADM, USN, "JMCIS" brief presented to the JMCIS Joint Requirements Working Group (JRWG), Dam Neck, Virginia Beach, Virginia, 19 October 1993.

10. Chevrier, John M., "JMCIS Introduction" Brief, Navy Research and Development (NRaD), 4 May 1994.

11. Science Applications International Corporation (SAIC), *JMCIS Version 2.1, (Sensitive Compartmented Information (SCI)), Security Requirements Document,* Revision 1, 22 April 1994.

12. Space and Naval Warfare Systems Command (SPAWAR), *Navy Tactical Command System - Afloat (NTCS-A) Project Overview*, brief given on 13 July 1993.

13. General Accounting Office, National Security Affairs Division, *DoD's Efforts Achieve Interoperability Among C3 Systems, GAO/IMTEC-89-57*, Government Printing Office, Washington, DC, April 1987.

14. The National Military Strategy Document (NMSD) for FY 1994-1999.

15. SECNAVINST 5239.2, *Department of the Navy Automated Information Systems (AIS) Security Program*, 15 November 1989.

16. Greer, Mark F., *A Sensitive Compartmented Information System Architecture for the Navy Tactical Command System-Afloat (NTCS-A)*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1991.

17. Science Applications International Corporation (SAIC), *JMCIS Version 2.1, (Sensitive Compartmented Information (SCI)), Concept of Operations and Security Analysis,* Internal Preliminary Draft In Progress, July 1994.

18. Mitchell, Curtis, CDR, USN, "Naval Electronic Combat Surveillance Systems", brief presented to the JMCIS Joint Requirements Working Group (JRWG), San Diego, California, 25 April 1994.

19. Pfleeger, Charles P., "Security in Computing," *Prentice Hall*, 1989.

20. Defense Intelligence Agency, "Department of Defense Intelligence Information System (DoDIIS) Developer's Guide", November 1993.

21. Russell, Deborah and G.T. Gangemi Sr., "Computer Security Basics," *O'Rielly and Associates, Inc.*, 1991.

22. DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)*, December 26, 1985.

23. Chokhani, Santosh, "Trusted Products Evaluation", *Communications of the ACM*, Vol. 35, No. 7, July 1992.

24. Shockley, W.R., Schell, R.R., and Thompson, M F., "The Importance of High Assurance Computers for Command, Control, Communications, and Intelligence Systems," *Proceedings of the Fourth Aerospace Computer Security Applications Conference*, pp.331-342, 12-16 December 1988.

25. Grant, Peter, and Riche, Robert, "The Eagle's Own Plume," *U.S. Naval Institute Proceedings*, v. 109/7/965, pp. 29-34, July 1983.

26. Schell, Roger R., "Computer Security: The Achilles' Heel of the Electronic Air Force," *Air University Review*, pp. 16-33, January-February 1979.

27. National Computer Security Center, "A Guide to Understanding Configuration Management in Trusted Systems, NCSC-TG-006, Version 1", *U.S. Government Printing Office*, 28 March 1988.

28. Inter-National Research Institute (INRI), *Security Shell Service Application Programmer's Interface (API), SPAWARSYSCOM SDE-API-SECURITY-2.0*, 15 March 1994.

29. National Computer Security Center, "Glossary of Computer Security Terms, NCSC-TG-004-88", *U.S. Government Printing Office*, 21 October 1988.

30. National Computer Security Center, "A Guide to Understanding Discretionary Access Control in Trusted Systems, NCSC-TG-003", *U.S. Government Printing Office*, 30 September 1987.

31. National Computer Security Center, "A Guide to Understanding Identification and Authentication in Trusted Systems, NCSC-TG-017, Version 1", *U.S. Government Printing Office*, 1 September 1991.

32. Department of Defense, "Password Management Guideline, CSC-STD-002-85", *U.S. Government Printing Office*, 12 April 1985.

33. Hinke, Thomas H. and Schaefer, Marvin, "Secure Data Management Systems", RADC-TR-75-266, Final Technical Report, November 1975.

34. National Computer Security Center, "A Guide to Understanding Audit in Trusted Systems, NCSC-TG-001, Version 2", *U.S. Government Printing Office*, 1 June 1988.

35. National Computer Security Center, "A Guide to Understanding Data Remanence in Automated Information Systems, NCSC-TG-025", *U.S. Government Printing Office*, September 1991.

36. National Computer Security Center, "A Guide to Understanding Object Reuse in Trusted Systems, NCSC-TG-018, Version 1", *U.S. Government Printing Office*, July 1992.

37. Fellows, Jon, et. al., "The Architecture of a Trusted Computing Base".

38. National Computer Security Center, "Trusted Network Interpretation, NCSC-TG-005, Version 1", *U.S. Government Printing Office*, 31 July 1987.

LIST OF ACRONYMS

ACL - Access Control List

ADP - Automatic Data Processing

AIS - Automated Information System

API - Application Programmer Interface

ASWOC - Anti-Submarine Warfare Operations Center (now TSC)

CCC - CINC Command Center

CINC - Command In Chief

COE - Common Operating Environment

COMSEC - Communications Security

COTS - Commercial Off-The-Shelf Software

CTAPS - Contingency Theater Automated Planning System

DAC - Discretionary Access Control

DBMS - Data Base Management System

DoD - Department of Defense

DoDIIS - Department of Defense Intelligence Information System

EWCM - Electronic Warfare Coordination Module

GOTS - Government Off-The-Shelf Software

JDISS - Joint Defense Intelligence Support Services

JMCIS - Joint Maritime Command Information System

JOTS - Joint Operational Tactical System

LAN - Local Area Network

MAC - Mandatory Access Control

NALCOMIS - Naval Aviation Logistics Command Management Information System

NAVSSI - Navigation Sensor System Interface

NCCS-A - Navy Command and Control System - Ashore

NIPS - NTCS-A Intelligence Processing System

NITES - NTCS-A Integrated Tactical Environmental Subsystem

NTCB - Network Trusted Computing Base

NTCCS - Navy Tactical Command Support System

NTCS-A - Navy Tactical Command and Control System - Afloat

NWSS - Navy WWMCCS Software Standardization

OSS - Operations Support System

RTE - Runtime Environment

SNAP - Shipboard Non-tactical ADP Program

TCB - Trusted Computer Base

TCSEC - Trusted Computer System Evaluation Criteria

TDA - Tactical Decision Aid

TIMS - Tactical Information Management System

TSC - Tactical Support Center (formerly ASWOC)

UB - Unified Build

WWMCCS - World Wide Military Command Center System

GLOSSARY

Access - (1) A specific type of interaction between a subject and an object that results in the flow of information from one to the other. (2) The ability and the means necessary approach, to store or retrieve data, to communicate with, or to make use of any resource of an ADP system.

Access Control - (1) The limiting of rights or capabilities of a subject to communicate with other subjects, or to use functions or services in a computer system or network. (2) Restrictions controlling a subject's access to an object.

Access Control List - (1) A list of subjects authorized for specific access to an object. (2) A list of entities, together with their access rights, which are authorized to have access to a resource.

Accountability - The quality or state which enables actions on an ADP system to be traced to individuals who may then be held responsible. These actions include violations and attempted violations of the security policy, as well as allowed actions.

Accreditation - the managerial authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, make on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements, e.g., TCSEC, for achieving adequate data security. Management can accredit a system to operate at a higher/lower level than the risk level recommended for the certification level of the system. If management accredits the system to operate at a higher level than is appropriate for the certification level, management is accepting the additional risk incurred.

Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD 5200.28-STD

Application Programmer Interface (API) - A programmer's guide which describes the JMCIS software libraries and how to write software modules which interface with the use the JMCIS software modules.

Approved Software - Software, while not delivered to developers by SPAWAR PD-60- as part of JMCIS, that has been tested and found to be compatible with the JMCIS environment. (An "approved products list" - UNIX, Motif, Oracle, Sybase, WordPerfect, etc.) In this context, approved software implies only that is has been tested and confirmed to work within the JMCIS environment. It does not imply that the software has been approved or authorized by any government agency for any specific project.

Audit Trail - (1) A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transaction forward to related records and reports and/or backwards from records and reports to their component source transactions. (2) Information collected or used to facilitate a Security Audit.

Authentication - (1) To establish the validity of a claimed identity. (2) To provide protection against fraudulent transactions by establishing the validity of message, station, individual, or originator.

Category - A grouping of objects to which an non-hierarchical restrictive label is applied (e.g., proprietary, compartmented information). Subjects must be privileged to access a category.

Certification - The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular system's design and implementation meet a set of specified security requirements.

Commercial Off-The-Shelf Software (COTS) - Software which is available commercially. Examples include a particular vendor's version of UNIX, X Windows, or Motif as well as standard products such as Oracle, Sybase, and Informix.

Common Operating Environment (COE) - In the context of JMCIS, the COE is the collection of COTS software, core services, and APIs required to build a Command Information System.

Communication Channel - The physical media and devices which provide the means for transmitting information from one component of a network to (one or more) other components.

Compartment - A designation applied to a type of sensitive information, indicating the special handling procedures to be used for the information and the general class of people who may have access to the information. It can refer to the designation of information belonging to one or more categories.

Compromise - A violation of the security system such that an unauthorized disclosure of sensitive information may have occurred.

Confidentiality - The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration Control - Management of changes made to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system.

Core - That minimum collection of software required for a Command Information System irrespective of the target mission area. This includes software comprising the runtime operating environment, software to receive and process military format messages, software to manage a track database, and software for generating tactical displays.

Covert Channel - A communications channel that allows a process to transfer information in a manner that violates the system's security policy. A covert channel typically communicates by exploiting a mechanism not intended to be used for communication. See Covert storage channel and Covert timing channel. Compare Overt channel.

Covert Storage Channel - A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel - A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.

Data Integrity - (1) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. (2) The property that data has not been exposed to accidental or malicious alteration of destruction.

Dedicated Security Mode - The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specific period of time. Compare Multilevel Security Mode, System High Security Mode.

Discretionary Access Control (DAC) - A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that: (a) A subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject; (b) DAC is often employed to enforce need-to-know; (c) Access control may be changed by an authorized individual. Compare to Mandatory Access Control.

Domain - The set of objects that a subject has the ability to access.

Dominated by (the relation) - A security level A is dominated by security level B if the clearance/classification in A is less than or equal to the clearance/classification in B and the set of access approvals (e.g., compartment designator) in A is contained in (the set relation) the set of access approvals in B (i.e., each access approval appearing in A also appears in B). Depending upon the policy enforced (e.g., non-disclosure, integrity) the definition of "less than or equal to" and "contained in" may vary. For example, the level of an object of high integrity (i.e., an object which should be modifiable by very trustworthy individuals) may be defined to be "less than" the level of an object of low integrity (i.e., an object which is modifiable by everyone).

Dominates (the relation) - security level B dominates security level A if A is dominated by B.

Electronic Warfare Coordination Module (EWCM) - A stand..one program originally intended to provided EW support. This program was canceled and its functionality was incorporated into NTCS-A.

Environment - In the context of JMCIS, the environment is all software that is running from the time the computer is rebooted until just after an operator logs in and the system is ready to respond to operator queries. This includes a standard environment consisting of the operating system, security, installation software, windowing environment, etc. The environment can be broken into two classes: a runtime environment and a software development environment.

Exploitable Channel - Any channel that is usable or detectable by subjects external to the Trusted Computing Base.

Government Off-The-Shelf Software (GOTS) - In general usage, software developed through funding by the US Government. In the context of JMCIS, the SPAWAR PD-60 developed software provided to developers for use in building a Command Information System. GOTS should not be confused with JOTS, even though they are largely the same software. GOTS should be thought of as a development environment for building applications such as JOTS. GOTS has been replaced with the JMCIS Superset.

Integrity - See data integrity and integrity policy.

Integrity Policy - A security policy to prevent unauthorized uses from modifying, viz., writing, sensitive information.

Joint Defense Intelligence Support Services (JDISS) - A system which combines imagery, communications, database, and work processing functions to provide automated intelligence support for deployed joint task forces. JDISS is being incorporated into JMCIS.

Joint Maritime Command Information System (JMCIS) - JMCIS is both a software superset and the name of a system. The total collection of software provide by SPAWAR PD-60 for building and fielding Command Information Systems is the JMCIS Superset. The superset includes components from UB, OSS, NTCS-A, and other development efforts. JMCIS is also the name used to refer to the Command Information System fielded by SPAWAR PD-60 at U.S. Navy sites.

Label - See Security Label and Sensitivity Label.

Least Privilege - This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Mandatory Access Control (MAC) - A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

Multilevel Device - A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed.

Multilevel Secure - A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.

Multilevel Security Mode - The mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present. Compare Dedicated Security Mode, System High Security Mode.

Naval Aviation Logistics Command Management Information System (NALCOMIS) - A system for performing afloat naval air station aircraft maintenance planning and production. NALCOMIS functionality is being incorporated in NTCSS.

Naval Tactical Command Support System (NTCSS) - An umbrella program combining the functionality of SNAP, MRMS, and NALCOMIS into a common software and hardware baseline. NTCSS is being designed to allow feeding of information to NTCS-A.

Navigation Sensor System Interface (NAVSSI) - A system for collecting navi sensor inputs and providing them to NTCS-A.

Navy Command and Control System - Ashore (NCCS-A) - An umbrella program managed by SPAWAR PD-60 for a Command and Control system for use by ashore intelligence centers. Built on top of UB and sometimes referred to as OSS, NCCS-A emphasizes database queries, message processing for reporting ship status and movements, and preparation of daily briefings for senior military planners. NCCS-A is being replaced b JMCIS.

Navy Tactical Command System - Afloat (NTCS-A) - An umbrella program managed by SPAWAR PD-60 for a Command and Control system for use by afloat tactical commanders. Built on top of UB, NTCS-A consolidates into one program several previously separate systems for track management (JOTS), database (NIPS), status board displays (TIMS), imagery (NIEWS), and assorted TDAs. NTCS-A is being replaced by JMCIS.

Navy WWMCCS Software Standardization (NWSS) - An upgrade of WWMCCS designed to provide Navy status of forces data. NWSS functionality has been incorporated into OSS.

Network Architecture - The set of layers and protocols (including formats and standards that different hardware/software must comply with to achieve stated objectives) which define a Network.

Network Component - A network subsystem which is evaluatable for compliance with the trusted network interpretations, relative to that policy induced on the component by the overall network policy.

Network Connection - A network connection is any logical or physical path from one host to another that makes possible the transmission of information from one host to the other. An example is a TCP connection. But also, when a host transmits an IP datagram employing only the services of its "connectionless" Internet Protocol interpreter, there is considered to be a connection between the source and the destination hosts for this transaction.

Network Reference Monitor - An access control concept that refers to an abstract machine that mediates all access to objects within the network by subjects with the network.

Network Security - The protection of networks and their services from unauthorized modification, destruction, or disclosure. Providing an assurance that the network performs its critical functions correctly and there are no harmful side-effects. Includes providing for information accuracy.

NTCS-A Integrated Tactical Environment Subsystem (NITES) - A subsystem of NTCS-A, built on top of UB, that combines oceanographic, weather, and environmental data.

NTCS-A Intelligence Processing System (NIPS) - The component of NTCS-A which manages database queries and certain message handling tasks. NIPS is similar in some respects to functionality contained in OSS, but uses the Sybase COTS package for database management.

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, etc.

Operations Support System (OSS) - A system built on top of UB that was specifically designed for use in ashore Navy intelligence centers. OSS emphasizes database queries and message processing for obtaining status of ships. OSS is sometimes incorrectly used synonymously with DSS (a software component of OSS) and is sometimes correctly referred to as NCCS-A (Navy Command and Control System - Ashore). OSS uses the Oracle database product.

Overt Channel - An overt channel is a path within a network which is designed for the authorized transfer of data.

Penetration - The successful violation of a protected system.

Read - A fundamental operation that results only in the flow of information from an object to a subject.

Reference Monitor Concept - An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Reliability - The extent to which a system can be expected to perform its intended function with required precision.

Runtime Environment - The portion of the software environment that is required to properly execute JMCIS applications.

Secrecy Policy - A security policy to prevent unauthorized users from reading sensitive information.

Security Architecture - The subset of computer architecture dealing with the security of the computer or network system.

Security-Compliant Channel - A channel is Security-Compliant if the enforcement of the network policy depends only upon characteristics of the channel either (1) included in the evaluation, or (2) assumed as a installation constraint and clearly documented in the Trusted Facility Manual.

Security Kernel - The hardware, firmware, and software elements of a Trusted Computing Base (or Network Trusted Computing Base partition) that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Level - The combination of hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Segment - A collection of one or more CSCIs (Computer Software Configuration Items) most conveniently manage as a unit. Segments are generally defined to keep related CSCIs together (UB core, DSS Tables, NSOF, Strikeplot, etc.) so that functionality may be easily included or excluded in a JMCIS variant.

Sensitivity Label - A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the NTCB as the basis for mandatory access control decisions.

Shipboard Non-tactical ADP Program (SNAP) - A system for performing afloat inventory and financial management. SNAP functionality is being incorporated into NTCSS.

Storage Object - An object that supports both read and write accesses.

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

System High - The highest security level supported by a system at a particular time or in a particular environment.

System High Security Mode - The mode of operation in which system hardware and software is only trusted to provide discretionary protection between users. In this mode, the entire system, to include all components electrically and/or stored. All system users in this environment must possess clearances and authorization for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and that caveats have been affixed.

System Low - The lowest security level supported by a system at a particular time or in a particular environment.

Tactical Decision Aids (TDAs) - A software module which serves as a support function to the basic Command Information System. JMCIS provides several TDAs which include satellite vulnerability calculations, radio wave propagation, closet point of approach calculations, and water space management.

Tactical Information Management System (TIMS) - A system designed for use on afloat platforms to provide status information to tactical commanders. The status information is frequently presented as a result of a database query or in the form of dynamically updated status information displays (called ASTABS - Automatic Status Boards). TIMS connects to the NTCS-A LAN through a network of Personal Computers to a centralized TAC-3 server.

Tactical Support Center (TSC) - A Command Information System, currently built on top of UB and OSS, for supporting Anti-Submarine Warfare commanders.

Trap-door - A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e.g., special "random" key sequence at a terminal).

Trojan horse - A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a "blind copy" of a sensitive files for the creator of the Trojan Horse.

Trusted Channel - A mechanism by which two NTCB partitions can communicate directly. This mechanism can be activated by either of the NTCB partitions, cannot be imitated by untrusted software, and maintains the integrity of information that is sent over it. A trusted channel may be needed for the correct operation of other security mechanisms.

Trusted Computer System - A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Computing Base (TCB) - The totality of protection mechanisms within a computer system -- including hardware, firmware, and software-- the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Trusted Path - A mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base. This mechanism can only be activated by the person on the Trusted Computing Base and cannot be imitated by untrusted software.

Trusted Subject - A subject that is part of the TCB. It has the ability to violate the security policy, but is trusted not to actually do so. For example in the Bell-LaPadulla model a trusted subject is not constrained by the *-property and thus has the ability to write sensitive information into an object whose level is not dominated by the (maximum) level of the subject, but it is trusted to only write information into objects with a label appropriate for the actual level of the information.

Unified Build (UB) - An environment, a set of development tools, documentation, and modules for building a Command Information System. Strictly speaking, UB is not a deliverable system to an end user, but is delivered to developers only for use in building an end system. UB grew out of a consolidation of Navy Afloat and Ashore requirements and is often used synonymously with GOTS and JOTS, and is sometime incorrectly referred to as JMCIS or an end user system.

User - Any person who interacts directly with a network system. This includes both those persons who are authorized to interact with the system and those people who interact without authorization (e.g., active or passive wiretappers). Note that "user" does not include "operators." "system programmers," "technical control officer," "system security officers," and other system support personnel. They are distinct from users and are subject to the Trusted Facility Manual and the System Architecture requirements. Such individuals may change the system parameters of the network system, for example by defining membership of a group. These individuals may also have the separate role of users.

Variant - A JMCIS software configuration loaded on a single CPU in the system. The concept is that while JMCIS as a whole represents a "superset," a variant is that subset installed on a single CPU for a specific mission area such as mission planning, battlegroup database management, or anti-drug support.

Virus - Malicious software, a form of Trojan horse, which reproduces itself in other executable code.

Write - A fundamental operation that results only in the flow of information from a subject to an object.

Write Access - Permission to write an object.

BIBLIOGRAPHY

Abrams, Marshall D. and Harold J. Podell, "Computer and Network Security," *IEEE Computer Society Press*, Washington, D.C., 1987.

Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, *Corporate Information Management for the 21st Century, A DoD Strategic Plan*, June 1994.

Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, *Memorandum for Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, and Directors of the Defense Agencies regarding Selection of Migration Systems*, December 1993.

Chevrier, John M., "JMCIS Introduction" Brief, Navy Research and Development (NRaD), 4 May 1994.

Chief of Naval Operations, *Minutes of the Joint Maritime Command Information System (JMCIS) Requirements Working Group (JWRG)*, October 1993.

Chokhani, Santosh, "Trusted Products Evaluation", *Communications of the ACM*, Vol. 35, No. 7, July 1992.

Copernicus Architecture, *Phase 1:Requirements Definition*, 1991.

C4 Architecture Integration Division (J6I) J6, The Joint Staff, *Committed, Focused, and Needed, C4I For The Warrior*, Government Printing Office, Washington, DC, 1993.

Dearborn, Rebecca D., and Morales, Robert C., *An Overview of the Copernicus C4I Architecture*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1992.

Defense Intelligence Agency, "Department of Defense Intelligence Information System (DoDIIS) Developer's Guide", November 1993.

Denning, Peter J., "Computers Under Attack," *ACM Press*, 1990.

Department of Defense, "Password Management Guideline, CSC-STD-002-85", *U.S. Government Printing Office*, 12 April 1985.

Deputy Secretary of Defense, *DoD Directive 4630.5 - Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 1992.

DoD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988.

DoD Intelligence Information Systems Developer's Guide

DoD 5200.28-M, *ADP Security Manual--Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems*, 24 May 1979.

DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 26, 1985.

Fellows, Jon, Hemenway, Judy, Kelem, Nancy, and Romero, Sandra, "The Architecture of a Trusted Computing Base", *Proceedings of the 7th DoD/NBS Computer Security Conference, 1984.*

Gasser, Morrie, "Building a Secure Computer System," *Van Nostrand and Rienhold*, 1987.

General Accounting Office, National Security Affairs Division, *DoD's Efforts Achieve Interoperability Among C3 Systems*, Government Printing Office, Washington, DC, April 1987.

Gauss, John A, RADM, USN, "JMCIS" brief presented to the JMCIS Joint Requirements Working Group (JRWG), Dam Neck, Virginia Beach, Virginia, 19 October 1993.

Grant, Peter, and Riche, Robert, "The Eagle's Own Plume," *U.S. Naval Institute Proceedings*, v. 109/7/965, pp. 29-34, July 1983.

Greer, Mark F., *A Sensitive Compartmented Information System Architecture for the Navy Tactical Command System-Afloat (NTCS-A)*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1991.

Hamblen, Diane, "Copernicus," *CHIPS*, January 1992.

Hinke, Thomas H. and Schaefer, Marvin, "Secure Data Management Systems", RADC-TR-75-266, Final Technical Report, November 1975.

Inter-National Research Institute, Inc., *Joint Maritime Command Information System (JMCIS) Common Operating Environment (COE)*, Rev 1.4, February 1994.

Inter-National Research Institue, Inc., *Security Shell Service Application Programmer's Interface (API) for the Unified Build (UB) Software Development Environment (SDE)*, December 1993.

Inter-National Research Institue, Inc.,*Unified Build 2.0 Security Manager's Guide*, March 1994.

Lobel, Jerome, "Foiling the System Breakers," *McGraw-Hill, Inc.*, 1986.

Mitchell, Curtis, CDR, USN, "Naval Electronic Combat Surveillance Systems", brief presented to the JMCIS Joint Requirements Working Group (JRWG), San Diego, California, 25 April 1994.

National Computer Security Center, "A Guide to Understanding Audit in Trusted Systems, NCSC-TG-001, Version 2", *U.S. Government Printing Office*, 1 June 1988.

National Computer Security Center, "A Guide to Understanding Discretionary Access Control in Trusted Systems, NCSC-TG-003", *U.S. Government Printing Office*, 30 September 1987.

National Computer Security Center, "Glossary of Computer Security Terms, NCSC-TG-004-88", *U.S. Government Printing Office*, 21 October 1988.

National Computer Security Center, "Trusted Network Interpretation, NCSC-TG-005, Version 1", *U.S. Government Printing Office*, 31 July 1987.

National Computer Security Center, "A Guide to Understanding Identification and Authentication in Trusted Systems, NCSC-TG-017, Version 1", *U.S. Government Printing Office*, 1 September 1991.

National Computer Security Center, "A Guide to Understanding Object Reuse in Trusted Systems, NCSC-TG-018, Version 1", *U.S. Government Printing Office*, July 1992.

National Computer Security Center, "Security Testing and Test Documentation, NCSC-TG-023 Version 1", *U.S. Government Printing Office*, July 1993.

National Computer Security Center, "A Guide to Understanding Data Remanence in Automated Information Systems, NCSC-TG-025", *U.S. Government Printing Office*, September 1991.

National Computer Security Center, "Security Features User's Guide, NCSC-TG-026 Version 1", *U.S. Government Printing Office*, September 1991.

Pfleeger, Charles P., "Security in Computing," *Prentice Hall*, 1989.
Rich, Lyford D., *Unix Security: A Penetration Analysis of Navy Systems*, Master's Thesis, Naval Postgraduate School, Monterey, California, December 1992.

Russell, Deborah and G.T. Gangemi Sr., "Computer Security Basics," *O'Rielly and Associates, Inc.*, 1991.

Science Applications International Corporation (SAIC), *JMCIS Version 2.1, (Sensitive Compartmented Information (SCI)), Concept of Operations and Security Analysis*, Internal Preliminary Draft In Progress, July 1994.

Science Applications International Corporation (SAIC), *JMCIS Version 2.1, (Sensitive Compartmented Information (SCI)), Security Requirements Document*, Revision 1, 22 April 1994.

Space and Naval Warfare Systems Command (SPAWAR), *Navy Tactical Command System - Afloat (NTCS-A) Project Overview*. brief given on 13 July 1993.

Schell, Roger R., "Computer Security: The Achilles' Heel of the Electronic Air Force," *Air University Review*, pp. 16-33, January-February 1979.

SECNAVINST 5239.2, *Department of the Navy Automated Information Systems (AIS) Security Program*, 15 November 1989.

Shockley, W.R., Schell, R.R., and Thompson, M.F., "The Importance of High Assurance Computers for Command, Control, Communications, and Intelligence Systems," *Proceedings of the Fourth Aerospace Computer Security Applications Conference*, pp.331-342, 12-16 December 1988.

Shirley, Lawrence Jay, *Non-Discretionary Security By Validation*, Master's Thesis, Naval Postgraduate School, Monterey, California, 1981.

Sterne, Daniel F., "On the Buzzword"Security Policy"", *Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 219-230, May 20-22, 1991.

The National Military Strategy Document (NMSD) for FY 1994-1999.

Tuttle, Jerry O., "OPNAV N6" brief presented to the JMCIS Joint Requirements Working Group (JRWG), Dam Neck, Virginia Beach, Virginia, 19 October 1993.

Walsh, Edward J., "Navy Aims at Joint Operations Roles and Economies for C^4I," *Sea Power*, , April 1994.

INITIAL DISTRIBUTION LIST

		Number of Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 52 Naval Postgraduate School Monterey, California 93943-5101	2
3.	Systems Management, Code 36 Naval Postgraduate School Monterey, California 93943-5002	1
4.	Professor Carl R. Jones, Code SM/JS Department of Systems Management Naval Postgraduate School Monterey, California 93943-5002	1
5.	Professor Cynthia E. Irvine, Code CS/IC Department of Computer Science Naval Postgraduate School Monterey, California 93943-5002	1
6.	Commander Naval Security Group Command 3801 Nebraska Ave. NW Washington, DC 20393-5210 ATTN: CDR Steve Paluszek - Code GX	1
7.	Professor Gary Porter, Code CC/PO C3 Academic Group Naval Postgraduate School Monterey, California 93943-5002	1

8. Commanding Officer 2
Naval Security Group Activity Pensacola
475 Jones Street
Corry Station
Pensacola, FL 32511-5204
ATTN: LT Mark T. Weatherford